AVG

ALGEMENE VERORDENING GEGEVENSBESCHERMING

MAAS

FAQ

Versie 3.8
02 september 2024

"Before I write my name on the board, I'll need to know how you're planning to use that data."

INHOUDSOPGAVE

Inleiding

Wat is de reikwijdte van deze FAQ?
Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht. Vrijwel alle verwerkingen van persoonsgegevens door en voor MAAS vallen onder deze Europese verordening, met directe werking als nationale wetgeving.
Uitzondering is de Verklaring Omtrent Gedrag, deze verwerkingen van persoonsgegevens voor MAAS valt onder de Wet justitiële en strafvorderlijke gegevens. Deze wet is in 2018 aangepast om te voldoen aan de Europese richtlijn 2016/680 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens.

Waarom deze FAQ?
Aan de hand van de volgende FAQ geeft MAAS uitleg over deze wet en wat dit voor MAAS medewerkers en de relaties van MAAS betekent. Veel uitleg wordt ook gegeven door de Autoriteit Persoonsgegevens. In dat geval begint een hoofdstuk met de vraag: *Wat zegt de Autoriteit Persoonsgegevens over [naam onderwerp]?*

Let op:
Dit document is enkel bedoeld als naslagwerk. Hieraan kunnen uitdrukkelijk geen rechten worden ontleend. De antwoorden in dit document zijn richtlijnen. Iedere situatie is anders waardoor de antwoorden mogelijk niet op jouw/ uw situatie van toepassing zullen zijn.

Wat als ik nog vragen heb en het antwoord niet kan vinden in dit document of bij de Autoriteit Persoonsgegevens?
MAAS tracht zo compleet mogelijk te zijn in het beantwoorden van mogelijke vragen. Mocht het antwoord op uw vraag er niet bij staan, dan kun je contact opnemen met je leidinggevende. Klantenvragen altijd eerst via de reguliere contacten te laten verlopen, zoals accountmanager of MAAS servicedesk. Deze zal contact opnemen met de Functionaris Gegevensbescherming van MAAS.

Wat is de waarde van informatie op Internet?
In het kader van de AVG is er ook veel documentatie te vinden op internet. Gebruik deze informatie als leidraad, maar zie dit niet als absolute waarheid die toepasbaar is in MAAS of voor MAAS. een advies of document kan vaak maar één keer voor een specifieke situatie worden gebruikt. Gebruik je hetzelfde advies of document voor een andere situatie, dan blijkt dat het niet meer voldoet. Laat juridische informatie en documenten daarom controleren door professionals.

Eerste hulp bij privacy
https://hulpbijprivacy.nl/#waarom-privacy

1. Autoriteit Persoonsgegevens. Algemene Verordening Gegevensbescherming

Wat zegt de Autoriteit Persoonsgegevens in het algemeen over de AVG?
Zie: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg

Wat is de AVG?
De AVG is de Algemene Verordening Gegevensbescherming. Deze – Europese – privacywetgeving vervangt sinds 25 mei 2018 de Nederlandse Wet bescherming persoonsgegevens (Wbp). De AVG is strenger dan de Wbp. Zo worden organisaties die persoonsgegevens verwerken strenger gecontroleerd en is er meer aandacht voor de rechten van de personen wiens gegevens worden verwerkt.

Wat betekent GDPR?
De afkorting GDPR betekent General Data Protection Regulation. De AVG is de Nederlandstalige versie van de GDPR.

Is er verschil tussen de AVG en de GDPR?
Nee, AVG staat voor Algemene Verordening Gegevensbescherming en is de Nederlandse benaming voor dezelfde wet in het Engels: General Data Protection Regulation (GDPR).

Wat is het gevolg van de invoering van de AVG voor MAAS en haar klanten?
Voldoen aan de van toepassing zijnde wet- en regelgeving is een vast en belangrijk onderdeel binnen MAAS. MAAS voldoet aan de EU en NL wet- en regelgeving en heeft sinds de introductie van de AVG in 2016 eventuele noodzakelijke aanpassingen in procedures beoordeeld en ingevoerd.

Is de AVG allesomvattend?
Nee, er is sprake van gelaagdheid in wetgeving. Op Europees niveau geldt de AVG. Deze kent algemene bepalingen en beginselen, maar geeft ook mogelijkheden voor de lidstaten van de Europese Unie om bepaalde zaken op nationaal niveau af te regelen. Deze aangelegenheden worden in Nederland uitgewerkt in de Uitvoeringswet AVG. Om meerdere redenen was er een bijbehorende Nederlandse wet nodig: om het bestaan en de positie van de Autoriteit Persoonsgegevens te regelen;
om (grote!) keuzeruimte die de AVG laat in te vullen, bijvoorbeeld ten aanzien van bijzondere persoonsgegevens; om de Wet bescherming persoonsgegevens (Wbp) in te trekken.
Verder worden in sectorspecifieke wetten concrete grondslagen voor verwerking van bijzondere persoonsgegevens (zoals gegevens over gezondheid) opgenomen, en worden sectorspecifieke uitzonderingen en afwijkingen opgenomen. Daarbij kan gedacht worden aan de Wet op de geneeskundige behandelingsovereenkomst en de Zorgverzekeringswet.

Op welke data is de AVG van toepassing?
AVG is van toepassing op alle persoonsgegevens en gegevens die individueel of in onderlinge samenhang herleidbaar zijn tot een individu. Dat kan variëren van een naam, een foto, een e-mailadres, bankgegevens, posts op sociale media, medische gegevens, tot een IP-adres, een MAC-adres en tracking cookies van je website. Dit is nieuw ten opzichte van de oude privacywetgeving. Je moet dus grip krijgen op alle contactmomenten, kanalen en gegevens die worden vastgelegd. De regelgeving strekt zich uit tot alle persoonsgegevens die tot individuen herleidbaar zijn en maakt

geen onderscheid tussen persoonlijke en zakelijke relaties (B2B), zowel van kandidaten als van (potentiële) opdrachtgevers.

Op welke gegevens is de AVG niet van toepassing?
De AVG is niet van toepassing op anonieme data of geanonimiseerde data, waarbij de gegevens die niet meer terug herleidbaar zijn tot individuen.
Voor persoonlijk of huishoudelijk gebruik is de AVG niet van toepassing. Je moet er daarbij voor zorgen dat de informatie alleen zichtbaar is voor een beperkte kring mensen, zoals familieleden of vrienden. De gegevens mogen dus niet openbaar zijn voor iedereen (ook niet voor 'vrienden van vrienden' op Facebook). Via zoekmachines mogen de gegevens ook niet te vinden zijn.

Is de AVG alleen van toepassing op digitale bestanden?
De AVG bepaalt de regels voor het verwerken van persoonsgegevens. Omdat dit tegenwoordig grotendeels digitaal gebeurt wordt papier al snel vergeten. Dat is onterecht, want het is voor de AVG niet relevant of je gegevens digitaal of analoog verwerkt . Als je persoonsgegevens verwerkt dan is de AVG daarop van toepassing. Zo kan een datalek bijvoorbeeld ook plaatsvinden als vertrouwelijke papieren documenten verloren gaan of in verkeerde handen komen. Ook bij een verzoek tot inzage in verwerkte persoonsgegevens mag je papieren documenten niet vergeten.
https://ddma.nl/mythes/

Is de AVG niet relevant als je gegevensbeveiliging goed in orde is?
Door de naam Algemene Verordening Gegevensbescherming wordt vaak onterecht aangenomen dat het een beveiligingsvraagstuk is. Het gaat echter om veel meer. Security is maar een beperkt onderdeel van de nieuwe wet. Het gaat om de bescherming van persoonsgegevens in de breedste zin van het woord. Maak daarom niet de fout om de AVG te zien als een IT/Security vraagstuk. Het is relevant voor alle personen die binnen je organisatie met persoonsgegevens werken.
https://ddma.nl/mythes/

2. Autoriteit Persoonsgegevens. Hulp bij Privacy en Guidelines

Wat zegt de AP over hulp bij privacy?
https://hulpbijprivacy.nl/

Over welke onderwerpen is hulp van de AP al beschikbaar voor ondernemers?

- https://www.hulpbijprivacy.nl/#voor-ondernemers-zieke-medewerkers
- https://www.hulpbijprivacy.nl/#voor-ondernemers-verwerkers
- https://www.hulpbijprivacy.nl/#voor-ondernemers-privacy
- https://www.hulpbijprivacy.nl/#voor-ondernemers-datalekken

Welke hulp van de AP beschikbaar voor iedereen?

- https://www.hulpbijprivacy.nl/#voor-iedereen

Wat zegt de AP over guidelines?
De Autoriteit Persoonsgegevens (AP) publiceert samen met de andere Europese privacytoezichthouders guidelines die bepaalde onderwerpen uit de AVG verduidelijken.
https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/avg-guidelines

Op welke vragen geeft de AP sinds medio 2020 geen antwoord (meer)?
Eenvoudige FAQ. AP heeft de FG's de eerste 2 jaar na de komst van de AVG bij de hand genomen en begeleid omdat we iedereen zo goed mogelijk wilden helpen met opstarten. Eerder hielpen we FG's nog weleens op weg met het doorsturen van linkjes naar pagina's op AP website met informatie over bepaalde AVG-uitgangspunten. Nu vraagt AP aan de FG om zelf die informatie op te zoeken. De AVG kent veel open normen. We krijgen dan ook vaak oplossingen voorgelegd met de vraag "Mag dit van de AVG?" Zo'n vraag om een 'stempel van de AP' is heel begrijpelijk, maar zonder een uitgebreide analyse van de situatie kan de AP dat niet beoordelen. Wat een passende beveiliging is, verschilt per situatie. Daarom zijn die normen ook open gehouden. De betrokken FG kent de case van A tot Z en kan én moet de wet kunnen toepassen. In het verleden konden FG's nog wel eens met ons sparren over waar zij op moesten letten, zoals bij het beoordelen van een verwerkingsovereenkomst. Nu zal de AP vaker zeggen: hiermee moet je als FG zelf aan de slag.

Met welke vragen kan de FG nog wel terecht bij de AP?
AP denkt nog steeds graag mee over complexe AVG-dilemma's waarbij je als FG alles al gedaan hebt om tot een antwoord te komen. En er bijvoorbeeld door tegenstrijdigheden in de regelgeving en/of de betreffende context niet uitkomt. Deze vragen zien we als belangrijke signalen over wat er speelt in een sector en hoe lastig de afwegingen zijn waarover de FG de verwerkingsverantwoordelijke adviseert. In het geval je als FG twijfelt over de invulling van je rol in relatie tot de verwerkingsverantwoordelijke - en hierdoor in een lastige situatie komt - kan je ook altijd contact opnemen met de AP.

En waar kan de FG dan nu terecht met dit soort vragen?
We zien dat FG's steeds beter hun weg weten te vinden en bijvoorbeeld onderling sparren met collega-FG's via koepel overleggen en samenwerkingsverbanden. En zo nodig een juridisch adviesbureau inschakelen of zichzelf bijscholen. Dat is ook veel logischer dan deze vragen aan de toezichthouder voorleggen. Een advies van de toezichthouder is immers niet vrijblijvend. Bovendien kunnen wij over concrete casussen geen advies geven zonder alle ins en outs te kennen. Gelukkig zijn er inmiddels meer dan 10.000 FG's aangemeld die de ins en outs van hun specifieke situatie wel kennen.

Maar waarom kan de AP geen advies geven over concrete casussen?
Die vraag krijgt de AP vaker. AP maakt dan wel eens de vergelijking met de Wegenverkeerswet. Stel: je wilt voor het eerst de weg op met een aanhangwagen, waar ook nog eens van alles uitsteekt. Je legt alles klaar, vlaggen en linten en dergelijke. Je moet vervolgens zelf uitvogelen hoe je één en ander bevestigt. Het is jouw verantwoordelijkheid om aan de regels te voldoen en om te bepalen of je ermee gaat rijden of niet. Je kunt niet de politie bellen en zeggen 'Ik denk dat het wel goed gegaan is, maar willen jullie voor de zekerheid alles even nalopen?" Het is begrijpelijk dat je van iemand een check wilt, maar de toezichthouder is niet de aangewezen instantie. Dat is eigenlijk met de AVG net zo. Alleen begrijpen wij natuurlijk wel dat FG's in de beginperiode van de AVG ons als aanspreekpunt zagen. Daarom hebben wij ook dat extra stapje gedaan om iedereen zo goed mogelijk in het zadel te helpen. Het doel was deze nieuwe beroepsgroep een kickstart te geven en aan het niveau van de vragen af te lezen, is dat zeker gelukt!

3. Autoriteit Persoonsgegevens. Bevoegdheden

Wat zegt de AP over bevoegdheden?
https://autoriteitpersoonsgegevens.nl/nl/over-de-autoriteit-persoonsgegevens/taken-en-bevoegdheden

Bron (geraadpleegd 25 september 2019):
https://www.hekkelman.nl/blog/overheidszaken/avg-ap-deel-6-wees-voorbereid-op-onderzoek-van-de-ap/

Wat zijn de onderzoeksbevoegdheden van de AP?
De onderzoeksbevoegdheden van de AP zijn te vinden in de Algemene Verordening Gegevensbescherming (AVG), de Nederlandse uitvoeringswet bij de AVG (UAVG) en de Algemene wet bestuursrecht (Awb).
De AP kan op allerlei manieren informatie opvragen, bijvoorbeeld per brief, e-mail of telefonisch. Ook kan de AP bij een organisatie aangeven dat zij vindt dat sprake is van een vermeende inbreuk op de AVG. Verder kan de AP volgens de AVG zogenoemde 'gegevensbeschermingscontroles' uitvoeren. Wat hieronder precies wordt verstaan zal nog moeten blijken. Ook kan de AP zaken en vervoermiddelen onderzoeken en monsters nemen.
Een onderzoek van de AP kan zien op handhaving, maar ook voor andere doeleinden kan zij onderzoek uitvoeren. Bijvoorbeeld als zij aanbevelingen of informatie over een bepaald onderwerp wil verstrekken. Lees bijvoorbeeld over de onderzoeken die ik in een eerdere blogpost heb besproken.
De AP gebruikt daarnaast andere instrumenten om toe te zien op naleving van de AVG. Zo kan zij een organisatie uitnodigen voor het verstrekken van inlichtingen. Ook stuurt de AP regelmatig brieven aan brancheorganisaties met haar standpunt en advies ten aanzien van een specifiek onderwerp (zoals de brief die de AP in 2017 aan de VNG stuurde over het openbaar maken van stukken).
Stel, de AP staat op de stoep, dan zijn de belangrijkste bevoegdheden hieronder aangegeven.

Wat betekent de AP bevoegdheid: Vorderen van inlichtingen en vorderen van inzage in zakelijke gegevens of bescheiden?
De AP heeft bevoegdheid om personen binnen je organisatie te vragen om inlichtingen te geven over de wijze waarop de organisatie omgaat met persoonsgegevens. De AP kan ook toegang verkrijgen tot computers of andere devices (zoals tablets en telefoons) waarmee persoonsgegevens worden verwerkt. De AP kan ook kopieën van stukken opvragen. Denk bijvoorbeeld aan het verwerkingsregister, het datalekkenregister en de informatie die je aan betrokkenen verstrekt.

Wat betekent de AP bevoegdheid: Bevoegdheid tot binnentreden (zonder toestemming)?
De AP heeft de bevoegdheid om bedrijfsruimten en woningen te betreden zonder toestemming. Deze bevoegdheid is niet grenzeloos: de AP dient zich bij deze vergaande bevoegdheid namelijk te houden aan de Algemene wet op het binnentreden.
Dit betekent onder andere dat de AP een machtiging moet hebben van de rechter-commissaris en een verslag moet maken van het binnentreden. Als ze een woning binnen willen treden, moet de specifieke ambtenaar ook nog een uitdrukkelijke en bijzondere volmacht hebben van de AP. Als de ambtenaren aangeven van deze bevoegdheid gebruik te maken, zullen ze deze dus moeten kunnen tonen.

Wat betekent de AP bevoegdheid: Verplichting tot medewerking?
Iedere organisatie is verplicht om medewerking te verlenen als de AP gebruik maakt van haar onderzoeksbevoegdheden. Als de AP toegang gelast tot persoonsgegevens, informatie of bedrijfsruimten en je leeft dit niet na, dan bepaalt de AVG dat dit met maximaal € 20.000.000 beboet kan worden.
De AP heeft boetebeleidsregels vastgesteld waaruit blijkt op welke wijze de AP de hoogte van een boete berekent.
De boete op het niet naleven van een last van de AP valt in de zwaarste categorie. Gelet op de beleidsregels van de AP komt dat neer op een boete tussen € 450.000 en € 1.000.000!

Wat zijn begrenzingen van de AP onderzoeksbevoegdheden?
Het uitoefenen van de onderzoeksbevoegdheden wordt begrensd door een aantal verplichtingen voor de AP. Dit zijn de voornaamste verplichtingen:

1. Proportionaliteit: Een belangrijke beperking voor de uitoefening van haar bevoegdheden is dat de AP altijd de proportionaliteit in acht dient te nemen. Dat wil zeggen dat zij slechts gebruik mag maken van haar onderzoeksbevoegdheden voor zover dat noodzakelijk is om toezicht te kunnen houden op de naleving van de AVG en UAVG. Voorbeeld: stel dat de AP aangeeft onderzoek te doen naar de wijze waarop de organisatie omgaat met verzuimgegevens van werknemers. In dat geval is het niet noodzakelijk dat zij inzage van alle klant- en bedrijfsgegevens verkrijgt. Deze mag de AP dan ook niet vorderen. Doet de AP dat wel? Dan mag je de AP erop wijzen dat je moet kunnen volstaan met het verlenen van inzage in de registratiesystemen en documenten waarin de verzuimgegevens worden verwerkt.
2. Zwijgrecht: Als de AP een bevoegdheid uitoefent met het oog op het opleggen van een punitieve sanctie dient zij aan de organisatie mede te delen dat deze niet verplicht is tot antwoorden(ook wel de ‘cautie’ genoemd). Een voorbeeld van een punitieve sanctie is een boete.
   Als de AP op bezoek komt voor onderzoek, zal zij dit doen met het oog op het geven van een punitieve sanctie. Het zwijgrecht geldt dan, en de AP is verplicht om de cautie te geven. Mocht de AP de cautie niet geven, vraag dan specifiek naar het doel van het onderzoek.
   Let op! Het zwijgrecht geldt niet voor werknemers. In de praktijk betekent dit dat het zwijgrecht alleen geldt voor personen die namens de organisatie spreken (zoals bestuurders).
3. Algemene beginselen van behoorlijk bestuur: Ook moet de AP zich als toezichthouder houden aan de algemene beginselen van behoorlijk bestuur. Bij het uitvoeren van het onderzoek zijn belangrijke beginselen onder meer: het gelijkheidsbeginsel, het evenredigheidsbeginsel (zoals hiervoor al toegelicht), het motiveringsbeginsel en het verbod op misbruik van bevoegdheid. Zo zal de AP haar onderzoeksbevoegdheden volgens het gelijkheidsbeginsel op een consistente manier moeten inzetten.

Wees voorbereid op een bezoek van de AP: wat kun je regelen?
De AP heeft veel onderzoeksbevoegdheden, maar deze zijn niet onbegrensd. Het is daarom aan te raden om een duidelijk stappenplan te hebben voor als de AP langskomt. Om te voorkomen dat je onnodig veel prijsgeeft als de AP op de stoep staat, aanbeveling om het volgende te regelen:

1. Stel crisisteam vooraf samen. Vorm een crisisteam met in ieder geval medewerkers met kennis van de gegevensstromen, hoger leidinggevenden en een jurist en/of advocaat. Gelet op het zwijgrecht verdient het aanbeveling om in het crisisteam mensen te plaatsen die de organisatie mogen vertegenwoordigen.
2. Leg de taken binnen crisisteam vast. De taken en rolverdeling bij een bezoek van de AP moeten duidelijk zijn voor verschillende betrokken personen. Ook moeten zij op de hoogte

zijn van de verplichtingen van de AP. Het is verstandig om dit vast te leggen in een interne regeling en deze binnen de organisatie te verspreiden via e-mail of intranet.

3. Maak stappenplan voor de ontvangst: Zorg dat er voor de medewerkers van de receptie een stappenplan klaar ligt om te gebruiken wanneer ambtenaren van de AP zich daar melden. Laat de ambtenaren zich bij binnenkomst legitimeren en begeleid ze naar een aparte ruimte. Neem direct contact op met de aangewezen verantwoordelijke(n) uit het crisisteam en de advocaat.
4. Stel vragen aan de AP. De persoon uit het crisisteam die de ambtenaren ontvangt zal ten eerste om een afschrift moeten vragen van het doel en de grondslag van het onderzoek. Aan de hand daarvan kun je namelijk beoordelen of het optreden van de AP proportioneel is. Tevens kun je dan de personen met kennis van zaken over het betreffende onderwerp oproepen.
5. Stel vooraf een vragenlijst voor de AP op. Het is verstandig om van tevoren al een vragenlijst op te stellen met vragen die in ieder geval aan de AP gesteld moeten worden. Daarin staat bijvoorbeeld dat je moet vragen naar het doel en grondslag van het onderzoek en de afbakening van het onderzoek.
6. Ondersteun de AP inspecteurs tijdens het onderzoek. Gelet op de verplichting tot medewerking is het belangrijk om de AP inspecteurs medewerking te verlenen tijdens het onderzoek. Het is van belang dat je, eventueel bijgestaan door je advocaat, de AP inspecteurs ondersteunt in het onderzoek. Laat ze niet alleen door het gebouw lopen. Vraag de AP inspecteurs tijdens het onderzoek telkens om toe te lichten waarom zij bepaalde handelingen tijdens het bezoek noodzakelijk achten voor het onderzoek.
7. Zorg voor verslaglegging van het bezoek: Wie ondervragen de AP inspecteurs, waartoe krijgen AP inspecteurs inzage, van welke documenten nemen AP inspecteurs kopieën mee. Dit is van belang om goed te kunnen beoordelen of AP inspecteurs binnen hun bevoegdheden blijven.

4. Autoriteit Persoonsgegevens. Organisatie

Wat zegt AP over de eigen organisatie:
https://autoriteitpersoonsgegevens.nl/nl/over-de-autoriteit-persoonsgegevens/organisatie

Wat is de Autoriteit Persoonsgegevens (AP)?
De EU-landen hebben conform artikel 8, lid 3, van Handvest van de grondrechten van de EU nationale autoriteiten aangewezen die toezicht houden op de bescherming van persoonsgegevens. In Nederland is dat de Autoriteit Persoonsgegevens. Zie ook:
https://autoriteitpersoonsgegevens.nl/nl

Hoe gaat het toezicht van de AP in zijn werk?
Iedereen kan een klacht bij de AP indienen over een mogelijke overtreding. De AP is verplicht iedere klacht in behandeling te nemen. Een klacht kan een controlerend onderzoek tot gevolg hebben. Vervolgens hebben we een hele gereedschapskist aan instrumenten om te handhaven. Dat kan een waarschuwing zijn, maar ook een sanctie als een last of een boete. De boetebevoegdheden van de Autoriteit Persoonsgegevens zijn onder de AVG uitgebreid van vorm: DE AP hoeft niet te bewijzen dat er opzet in het spel is.
De AP kent ook systeemtoezicht. Dat is een vorm van tweedelijns toezicht, ofwel toezicht op het toezicht van de organisatie zelf. Systeemtoezicht maakt gebruik van het aanwezige interne toezicht in een organisatie, bijvoorbeeld in de vorm van een functionaris gegevensbescherming. Is het toezicht binnen een sector of organisatie goed geregeld met bijvoorbeeld gedragscodes en goede functionarissen gegevensbescherming? Dan zal de AP wat meer op afstand toezicht houden.

Wie controleert de AP op de handhaving van de AVG?
Organisaties die zich niet kunnen vinden in een besluit van de Autoriteit Persoonsgegevens, kunnen daartegen in bezwaar en beroep gaan. Een beslissing op bezwaar kan een partij uiteindelijk voorleggen aan de rechter. AP besluiten kunnen verstrekkende gevolgen hebben, dus het is goed dat daar een zorgvuldige rechtsgang bij hoort.

Wie houdt Europees toezicht op de nationale AP's?
Dat is de *European Data Protection Board* in het Nederlands het Europees Comité voor Gegevensbescherming (ECG)?

Wat is het Europees Comité voor gegevensbescherming (ECG)?
Het ECG is een EU-orgaan dat per 25 mei 2018 verantwoordelijk is voor de toepassing van de Algemene Verordening Gegevensbescherming (AVG). Het ECG bestaat uit het hoofd van elke gegevensbeschermingsautoriteit en de Europese Toezichthouder voor Gegevensbescherming (EDPS), of hun vertegenwoordigers. De Europese Commissie neemt zonder stemrecht deel aan de vergaderingen van het ECG. Het secretariaat van het ECG wordt verzorgd door de EDPS.
Het ECG staat centraal in het nieuwe landschap voor gegevensbescherming in de EU. Mede dankzij het comité zal de gegevensbeschermingswetgeving in de hele EU consistent worden toegepast en wordt doeltreffende samenwerking tussen gegevensbeschermingsautoriteiten gewaarborgd. De raad van bestuur zal niet alleen richtsnoeren uitvaardigen voor de interpretatie van belangrijkste begrippen van de AVG, maar zal ook bindende beslissingen moeten nemen over geschillen in verband met grensoverschrijdende verwerking, om uniforme toepassing van de EU-regels te waarborgen en te voorkomen dat eenzelfde zaak in verschillende rechtsgebieden mogelijk verschillend wordt behandeld.

5. Autoriteit Persoonsgegevens. Onderzoek

Wat zegt AP zelf over onderzoek?
De AP doet onderzoek naar de naleving van de privacywetgeving. Heeft de AP tijdens onderzoek overtredingen vastgesteld? Dan kan de AP onder meer een boete geven of een last onder dwangsom opleggen.
Het is niet altijd nodig om direct een officieel onderzoek te starten. De AP kan ook eerst een gesprek met een organisatie voeren of een brief sturen. Zo'n interventie kan al genoeg zijn om de overtreding te doen stoppen.

Bron (geraadpleegd 25 september 2019):

- https://www.dirkzwager.nl/kennis/artikelen/wat-het-verleden-ons-kan-leren-over-handhaving-door-de-autoriteit-persoonsgegevens/
- https://www.yoursafetynet.com/nl/autoriteit-persoonsgegevens/

Wat zelf te doen bij onderzoek door de AP?
Ontvangt u een brief of telefoontje van de Autoriteit Persoonsgegevens? Dan is het dus zaak daarop direct zeer adequaat te reageren. Juist door in de onderzoeksfase al aan de AP te laten zien dat er geen sprake is van overtreding van de wet, of dat er geen belang is bij verder onderzoek, verkleint u de kans straks ook op de website van de AP te staan of te maken te krijgen met handhaving door de AP.

Hoe gaat een onderzoek van Autoriteit Persoonsgegevens in zijn werk?
Wanneer de Autoriteit Persoonsgegevens een overtreding vermoedt, zal het schriftelijk de nodige informatie opvragen bij de verantwoordelijke. Aan de hand van die informatie beslist het orgaan of een onderzoek ter plaatse noodzakelijk is. Zo'n onderzoek ter plaatse kan een beter beeld geven van de exacte situatie. Zo'n onderzoek kan zowel aangekondigd als onaangekondigd plaatsvinden.

Wat doet de Autoriteit Persoonsgegevens met de uitkomsten van zo'n onderzoek?
De Autoriteit Persoonsgegevens stelt aan het hand van het onderzoek de bevindingen op in een voorlopig rapport. De onderzochte organisatie kan hierop reageren, waarna een definitief rapport volgt. Een dergelijk definitief rapport is in principe openbaar te raadplegen, tenzij de onderzochte organisatie bezwaar heeft aangetekend tegen openbaring van bepaalde delen. De onderzochte organisatie moet daarvoor wel goede redenen kunnen aanvoeren.

Wat doet de Autoriteit Persoonsgegevens wanneer een overtreding is geconstateerd?
Blijkt uit het rapport dat een organisatie inderdaad de privacywetgeving overtreedt, dan kan zij hen op de vingers tikken. Dat kan in de vorm van bijvoorbeeld een bindend advies. De Autoriteit Persoonsgegevens kan in zo'n advies diverse maatregelen verplicht stellen, zoals een betere cybersecurity of het invoeren van een scherper afgebakend privacybeleid. Organisaties moeten in een gesteld tijdsbestek 'de boel op orde' brengen. Gebeurt dat niet, dan kan de Autoriteit Persoonsgegevens een forse boete opleggen.

6. Autoriteit Persoonsgegevens. Melding datalek

Wat zegt AP zelf over meldingsplicht?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken?qa=datalek

Wel of niet melden?
Autoriteit Persoonsgegevens (AP) vindt het oprecht jammer wanneer organisaties het idee hebben dat een datalek melden een soort schuldbekentenis is. Een datalek kan namelijk iedereen overkomen. Wanneer je het datalek op tijd aan de AP meldt, en je de betrokkenen informeert als dat nodig is, heb je over het algemeen niets te vrezen. Wel is het belangrijk dat je laat zien dat je er alles aan doet om de schade te beperken en dat je herhaling wilt voorkomen. Het is vooral belangrijk om binnen 72 uur te melden. Zodat de AP kan controleren of je de juiste stappen en maatregelen hebt genomen. De AP heeft als hulpmiddel een lijst met voorbeelden van 'wel- en niet-meldplichtige' datalekken gepubliceerd. Daarnaast wordt AP vaak gevraagd om in concrete gevallen advies te geven over het al dan niet melden van een datalek. AP laat als toezichthouder deze afweging juist bij de verantwoordelijken zodat de FG de ruimte heeft de AVG-normen toe te passen op de specifieke situatie. De FG kent de organisatie en de aard van de gegevens als geen ander en kan de risico's dus veel beter inschatten. Zonder onderzoek kunnen wij daar geen uitspraken over doen. Dat is bij uitstek de expertise van de FG. bestuurders moeten zich realiseren dat AP ook onderzoek doet naar niet gemelde datalekken. AP kan er ook op andere manieren achter komen dat een datalek niet is gemeld, terwijl dat wel had gemoeten. En dat rekent AP een verwerkingsverantwoordelijke wél standaard zwaar aan."

Wat als een bestuurder besluit om een datalek – ondanks het advies van de FG - niet te melden?
Zorg dan dat je als FG hebt vastgelegd wat jouw advies was. De verwerkingsverantwoordelijke blijft namelijk verantwoordelijk voor de uitvoering van het privacy beleid. Dat mag de FG niet worden aangerekend.

Wie doet de melding?
Een ander dilemma waar FG's mee te maken hebben, is wie het datalek meldt bij de AP. Wat AP vaak ziet is dat FG's een datalek bij ons melden. Ik kan me wel voorstellen hoe dat in de praktijk gaat. Door gebrek aan capaciteit kan het zo zijn dat de FG de enige medewerker is met verstand van de AVG. Overigens mág je als FG wel een datalek melden namens je bestuur, maar het zou beter zijn om die dubbele pet te voorkomen. De verantwoordelijkheid voor het melden van een datalek ligt immers bij de verwerkingsverantwoordelijke en niet bij de FG.
Het is een boodschap die de AP vaker geeft. Als FG ben je niet verantwoordelijk voor de uitvoering van het privacy beleid. Je adviseert een organisatie over wat een gezond privacy beleid is en houdt daar toezicht op. Dat is een wezenlijk verschil.
AP raadt daarom aan om bij het opstellen van een intern datalekproces duidelijk vast te laten leggen wie de afweging maakt of een datalek gemeld moet worden, en wie de melding uiteindelijk doet.

7. Autoriteit Persoonsgegevens. Open normen

Wat zegt AP over Open Normen:
…

Hoe invulling geven aan naleving van de open normen?
De AVG bevat zoals gezegd een groot aantal open normen en geeft organisaties daarmee een zekere vrijheid om praktische invulling aan wettelijke verplichtingen te geven.
Eén van de taken van de FG is intern toezicht te houden op de naleving hiervan. Daarbij staat de afweging over het gebruik van persoonsgegevens 'zo weinig en zo veilig mogelijk' centraal. Maar af en toe zie ik vragen van FG's waarbij het erop lijkt dat zij door hun organisatie worden gevraagd om vooral op zoek te gaan naar de uiterste norm. Ogenschijnlijk met als doel te achterhalen hoe een organisatie nog nét binnen de grenzen van de wet kan blijven. Dat vind ik hartstikke zonde. Want wanneer je uitgaat van het zoeken naar de uiterste norm, wordt de ondergrens de streefnorm. Dat druist in tegen het uitgangspunt van de AVG.
Het is dus een uitdaging voor FG's om erop te wijzen dat organisaties bij elke verwerking juist een zo hoog mogelijk beschermingsniveau moeten nastreven.

Wat is de rol van een organisatie als verwerkingsverantwoordelijke bij de uitleg van open normen?
Als een organisatie verwerkingsverantwoordelijke is, dan is in principe de directie of het bestuur van deze organisatie verantwoordelijk voor het correct toepassen van de AVG.
De organisatie moet in deze rol voldoende kennis van en deskundigheid over de AVG hebben om de open normen te kunnen invullen. De organisatie moet immers een goede afweging maken. Deze kennis en deskundigheid horen ook bij de uitvoerende afdelingen en ondersteunende juridische of ICT-afdelingen aanwezig te zijn. En dus niet alleen bij de FG. Mist er kennis? Dan kan de organisatie ook extern advies inwinnen.
Het is aan te bevelen dat een organisatie die verwerkingsverantwoordelijkheid heeft, beleid opstelt of een standpunt inneemt over het invullen van de normen. Denk aan een visie of interne richtlijnen. Daarin staat bijvoorbeeld of de organisatie streeft naar maximale bescherming van de (privacy)belangen van de betrokkenen. Of enkel aan het minimaal voldoen aan de wet. Of ergens daartussenin. Zulk beleid helpt om naleving aan te tonen en helpt medewerkers die in de praktijk de normen moeten invullen. Bovendien zorgt beleid voor transparantie naar betrokkenen.

Wat is de rol van de FG bij de uitleg van open normen?
De FG kan een belangrijke rol spelen bij de vertaling van open normen naar de praktijk. Daarvoor moet de FG wel op tijd en naar behoren betrokken worden. Dat staat ook in de wet.
Praktijkvoorbeeld
MAAS schaft beveiligingscamera's aan. MAAS is daarmee verwerkingsverantwoordelijke. Deze casus begint met de vraag: wat is de verhouding tussen de bescherming van persoonsgegevens en het doel om de camera's op te hangen? De FG kan in dit beginstadium adviseren en de organisatie laten nadenken over wat noodzakelijk is. Kan de gemeente het doel bijvoorbeeld ook bereiken met nepcamera's? Moeten de beelden wel worden opgeslagen, en zo ja: hoe lang? Kan MAAS betrokkenen eerst om hun mening vragen?
Als alle feiten en omstandigheden duidelijk zijn, kan de FG adviseren over de verschillende scenario's. MAAS in de rol van verwerkingsverantwoordelijke maakt vervolgens een doordachte keuze. Daarbij moeten open normen worden ingevuld. Bijvoorbeeld op het gebied van dataminimalisatie, bewaartermijnen of de toegang tot en de beveiliging van de verzamelde beelden. Legt MAAS het advies van de FG naast zich neer? Dan is daarvoor een onderbouwing nodig.

Wordt de FG te laat of te beperkt betrokken?
Bijvoorbeeld doordat het bedrijfsproces al helemaal is ingericht, de DPIA al is geschreven en de camera's al zijn aangeschaft? Dan zal de rol van de FG maar klein kunnen zijn bij het adviseren over de open normen. Op dat moment kan de FG immers alleen nog toetsen en adviseren over de vraag of de organisatie bij de uitleg van de open norm niet onder het minimale beschermingsniveau is uitgekomen. En of de verwerking daarmee nog wel rechtmatig is. Zeker wanneer geen intern beleid of visie is ontwikkeld, kan de FG alleen nog toetsen aan algemene kaders zoals de AVG, guidelines van de EDPB en rechtspraak. Dat is een gemiste kans en kan problemen opleveren.
Als FG kunt je in je adviezen of het jaarverslag aangeven hoe dit proces gaat. Dit helpt ook in uw contact met de AP. En de AP kan de informatie gebruiken om haar taken beter uit te voeren.

Wat is het nut van open normen en de 5 W's?
Erwin Daverveld FG van de AP: De open normen in de AVG zijn echt nodig. Kijk maar naar de snelle (technologische) ontwikkelingen waarmee we te maken hebben, zoals algoritmes, AI, big data en 'internet of things'. De open normen zorgen onder andere voor de benodigde flexibiliteit en ruimte, zonder dat innovatie hoeft te stagneren. De omstandigheden veranderen, maar open normen kunnen worden blijven ingevuld. Dat zorgt voor duurzame wetgeving.
Open normen, zoals het noodzakelijkheidsbeginsel, geven de FG de kans om na te denken over een casus, de specifieke omstandigheden te beoordelen en adviezen te geven zodat verwerkingen van persoonsgegevens voldoen aan de AVG.
Dit doet u als FG door bijvoorbeeld de uit de journalistiek bekende 5 W (en 1H)-vragen te stellen:

1. Wie: van wie worden de persoonsgegevens verwerkt?
2. Wat: in welke categorieën vallen de persoonsgegevens? (let op minimale gegevensverwerking, dus welke soorten gegevens zijn strikt noodzakelijk?)
3. Wanneer: wat is de bewaartermijn? (let op opslagbeperking: u mag gegevens niet langer bewaren dan noodzakelijk voor uw doel)
4. Waarom: wat is het doeleinde en wat is de wettelijke grondslag? (rechtmatigheid, behoorlijkheid en transparantie)
5. Waar: waar worden de gegevens opgeslagen?
6. Hoe: op welke manier worden de gegevens verwerkt en is er geen minder ingrijpende manier mogelijk? (subsidiariteit)

Zou de AVG zijn dichtgetimmerd, dan heef u als FG weinig mogelijkheden en is het lastiger om een verwerking 'AVG-proof' te maken.
Tip:
Het helpt ook om een data protection impact assessment (DPIA) op te stellen, een voorafgaande raadpleging in te dienen bij de AP en om 'privacy by design' & 'privacy by default' toe te passen. Door op deze manier een zorgvuldige invulling te geven aan de open norm 'noodzakelijkheidsbeginsel', en neem je de organisatie en werknemers mee. Als bijvangst verhoogt dit het bewustzijn, waardoor de volwassenheid op het gebied van de AVG in de organisatie toeneemt. De open normen in de AVG zorgen er juist voor dat veel wel kan, als u altijd maar het hoogst mogelijke beveiligingsniveau nastreeft.

8. Autoriteit Persoonsgegevens – Toezicht op algoritme

Wat zegt de Autoriteit Persoonsgegevens toezicht op Algoritmes?

- https://www.autoriteitpersoonsgegevens.nl/themas/algoritmes-ai/coordinatie-toezicht-algoritmes-ai
- https://www.autoriteitpersoonsgegevens.nl/themas/algoritmes-ai/coordinatie-toezicht-algoritmes-ai/directie-coordinatie-algoritmes-dca
- https://autoriteitpersoonsgegevens.nl/nl/nieuws/toezicht-op-algoritmes
- https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/toezicht_op_ai_en_algoritmes.pdf

Wie coördineert toezicht op Algoritmes?
Per 2023 is de Autoriteit Persoonsgegevens (AP) gestart als coördinerende autoriteit voor het toezicht op algoritmes. De AP geeft invulling aan deze rol vanuit de nieuwe directie Coördinatie Algoritmes (DCA). De toewijzing van deze taak aan de AP komt voort uit de ambitie om bij de ontwikkeling en inzet van algoritmes publieke waarden en grondrechten beter te beschermen.

Wat is de focus van de Directie Coördinatie Algoritmes (DCA)?
De focus van de DCA ligt op het beter beschermen van publieke waarden en grondrechten. Zoals discriminatie en willekeur voorkomen en transparantie bevorderen. Verder kijkt de DCA naar eerlijkheid van algoritmes en het voorkomen van misleiding. De werkzaamheden van de DCA staan los van (de intensivering van) het AP-toezicht op algoritmes die persoonsgegevens verwerken.

9. Functionaris Gegevensbescherming (FG) - MAAS

Wat zegt de Autoriteit Persoonsgegevens over de FG?

- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/functionaris-voor-de-gegevensbescherming-fg
- https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtlijnen_fg.pdf

Wat is een Functionaris Gegevensbescherming FG?
Een Functionaris Gegevensbescherming (FG) houdt toezicht op de toepassing en naleving van de privacy(wetgeving). De FG ondersteunt MAAS bij de praktische vertaalslag van het wettelijke kader naar de praktijk. De FG verzamelt hierbij informatie over de gegevensverwerking binnen MAAS en gaat na in hoeverre deze verwerking voldoet aan wet- en regelgeving. Daarnaast is de FG contactpersoon voor MAAS, andere FG's en de Autoriteit Persoonsgegevens (AP).

Heeft MAAS een Functionaris Gegevensbescherming (FG)?
Ja, zie hiervoor het MAAS Privacy reglement.

Hoe kan ik de MAAS FG bereiken?
Wij verzoeken u om uw vragen altijd eerst via de reguliere contacten te laten verlopen, zoals uw accountmanager of onze servicedesk. Mocht uw vraag niet (voldoende) beantwoord zijn, dan zal onze Functionaris Gegevensbescherming contact met u opnemen. Indien nodig zal onze Functionaris Gegevensbescherming (FG) contact met uw FG opnemen.

Wat is de primaire taak van de FG?
De Functionaris Gegevensbescherming (FG) is er in eerste instantie om de interne organisatie te adviseren over de naleving van de AVG

- informatie verzamelen om verwerkingswerkzaamheden te identificeren;
- analyseren en controleren in hoeverre verwerkingswerkzaamheden aan de AVG voldoen; en
- de verantwoordelijke of de verwerker informeren, adviseren of aanbevelingen geven.

Welke vragen beantwoordt de FG?
De FG beantwoordt de vragen op het gebied van privacy conform de AVG.

Welke verschillende wettelijke taken heeft de FG?

1. informeren en adviseren van de verwerkingsverantwoordelijke of de verwerker en de werknemers die verwerken, over hun verplichtingen uit hoofde van de AVG en andere relevante wet- en regelgeving;
2. toezien op naleving van de AVG en andere relevante wet- en regelgeving en van het beleid van de verwerkingsverantwoordelijke of de verwerker met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
3. desgevraagd advies verstrekken met betrekking tot de gegevensbeschermingseffect-beoordeling en toezien op de uitvoering daarvan in overeenstemming met wetgeving;
4. samenwerken met de toezichthoudende autoriteit;
5. optreden als contactpunt voor de toezichthoudende autoriteit inzake met verwerking verband houdende aangelegenheden, met inbegrip voorafgaande raadpleging over verwerkingen met een hoog risico, en, waar passend, overleg plegen over enige andere aangelegenheid.

Wat zijn de kenmerken van een FG volgens de AVG:

- wordt aangesteld op basis van diens professionele kwaliteiten en inhoudelijke expertise van het recht en de praktijk
- is onafhankelijk in de uitvoering van zijn of haar taken en rapporteert rechtstreeks aan het management
- krijgt alle noodzakelijke middelen tot zijn of haar beschikking om het werk te kunnen doen;
- is gebonden aan geheimhouding
- kan andere taken vervullen, zolang deze niet tot een belangenconflict leiden
- ontvangt geen uitvoeringsinstructies van de verantwoordelijke en geniet ontslagbescherming; hij of zij kan niet worden ontslagen of beboet op grond van de uitvoering van zijn of haar taken

Hoe kan de Functionaris voor de Gegevensbescherming van Maas International B.V. de taken, verantwoordelijkheden en bevoegdheden onafhankelijk en zonder enige belemmering uitoefenen?

Vastgelegd in MAAS Reglement Functionaris voor de gegevensbescherming, zie http://intranet.maas.nl/wp-content/uploads/2018/06/2018.05.25-MAAS-Reglement-Functionaris-voor-de-gegevensbescherming.pdf

10. Functionaris Gegevensbescherming (FG) - Nationaal Register

Wat zegt de Autoriteit Persoonsgegevens over Nationaal Register voor FG's (NRFG)?
De AP houdt in een intern FG-register bij welke FG's er zijn aangemeld, zie:
https://www.autoriteitpersoonsgegevens.nl/de-ap-en-privacy/privacyverklaring-autoriteit-persoonsgegevens/privacyverklaring-als-fg

Wat zegt Digitale Overheid over NRFG?
https://www.digitaleoverheid.nl/nieuws/voortgang-register-voor-fgs/

Wat zeggen marktpartijen over NRFG?
https://outvie.nl/kennisbank/nationaal-register-functionarissen-gegevensbescherming-wat-betekent-het-nu-voor-fgs/

Wat zegt de beroepsvereniging over NRFG?
https://www.ngfg.nl/nieuws/flinke-reservering-in-begroting-2023-voor-fg-register

Wat is het Nationaal Register voor FG's?
Het NRFG is een openbaar register voor erkende FG's om hun kwaliteit te waarborgen. In de praktijk blijkt namelijk dat het inhoudelijke niveau en de positionering van de ruim 10.000 FG's in Nederland uiteenlopen. Een openbaar register zou kunnen zorgen voor een kwalitatieve impuls.

Waarom komt er een NRFG?
Een FG houdt toezicht op het gebied van gegevensbescherming binnen organisaties. De rol en taken van een FG zijn in grote lijnen wettelijk vastgelegd in de Algemene Verordening Gegevensbescherming (AVG). Het verzoek voor het register komt voort uit de wens om het toezicht op de verwerking van persoonsgegevens te versterken. Dit meldt Franc Weerwind, minister voor Rechtsbescherming, aan de Tweede Kamer. Door de positie van de FG verder te professionaliseren wordt een belangrijke stap gezet in het versterken van dat toezicht, ook voor overheidsorganisaties. En dit is in het belang van werkgevers, privacy professionals en van burgers.

Wat is de voortgang begin 2024 van het NRFG?
Het Centrum Informatiebeveiliging en Privacybescherming (CIP) heeft een verkenning naar de wenselijkheid en haalbaarheid van een openbaar register voor Functionarissen Gegevensbescherming (FG's) uitgevoerd. Op dit moment werkt CIP aan de praktische kant van het NRFG. Denk aan de toetsingscriteria en -procedure, de voorwaarden om toegelaten te worden tot het register en het beschermen van alle gegevens. De verwachting is dat het register in de loop van 2024 wordt opgericht en kan worden gebruikt. Het traject wordt in opdracht van het ministerie van Justitie en Veiligheid (JenV) uitgevoerd.

11. Functionaris Gegevensbescherming (FG) - Jurisprudentie

Bronnen:

- https://www.stradalex.com/nl/sl_news/document/sl_news_article20220629-3-nl
- Hof van Justitie van de Europese Unie - Arrest van het Hof (Eerste kamer) van 22 juni 2022 (ECLI:EU:C:2022:495)
- Art. 38. - Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (Voor de EER relevante tekst) (PB. L 119, 4 mei 2016, p. 1)

Waaraan moet een nationale regeling voldoen ten aanzien van ontslag van een FG?
Een nationale regeling kan bepalen dat een functionaris voor gegevensbescherming alleen om ernstige redenen kan worden ontslagen, zelfs indien het ontslag geen verband houdt met de uitvoering van de taken van de functionaris. Het is echter noodzakelijk dat deze regeling de verwezenlijking van de doelstellingen van de GDPR niet in gevaar brengt.

Wat is de overweging van het Hof van Justitie van de Europese Unie over een nationale regeling ten aanzien van ontslag van een FG?
Het ontslag van de functionaris voor gegevensbescherming is verboden, maar niet absoluut
Het Hof van Justitie van de Europese Unie heeft op 22 juni 2022 een arrest gewezen over de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens.

Het verzoek om een prejudiciële beslissing betreft de uitlegging en de geldigheid van artikel 38, lid 3, tweede zin, van de Algemene Verordening Gegevensbescherming (AVG of GDPR).

In de onderneming L. vervult de heer LH de functie van functionaris voor gegevensbescherming. Hij is ontslagen met opzegging. De geldigheid van dit ontslag wordt betwist. Het Hof van Justitie wordt gevraagd of artikel 38, lid 3, tweede zin, van de GDPR zich verzet tegen een nationale regeling die bepaalt dat een functionaris voor gegevensbescherming die deel uitmaakt van zijn personeel, slechts om ernstige redenen kan ontslaan worden, zelfs indien het ontslag geen verband houdt met de uitoefening van de functie van deze functionaris.

Artikel 38, lid 3, van de GDPR bepaalt dat de functionaris voor gegevensbescherming niet van zijn taken mag worden ontheven of mag worden gestraft voor de uitvoering van zijn taken.

Deze bepaling stelt een grens die erin bestaat dat het verboden is deze functionaris te ontslaan om redenen die verband houden met de uitvoering van haar/zijn taken, waaronder het toezicht op de naleving van de wetgeving van de Unie of van de lidstaten inzake gegevensbescherming en van de interne voorschriften inzake de bescherming van persoonsgegevens.

Doel van deze bepaling is functionarissen voor gegevensbescherming in staat te stellen hun taken en verplichtingen in volledige onafhankelijkheid uit te voeren.

Om de functionele onafhankelijkheid van de functionaris voor gegevensbescherming te garanderen, mag die geen instructies krijgen voor de uitvoering van deze taken en moet die rechtstreeks verslag uitbrengen aan het hoogste bestuursniveau van de verwerkingsverantwoordelijke of verwerker van persoonsgegevens.

Artikel 38, lid 3, tweede zin, van de GDPR moet worden gezien als primair gericht op het behoud van de functionele onafhankelijkheid van de functionaris en dus op het waarborgen van de doeltreffendheid van de bepalingen van de GDPR.

Deze bepaling is niet bedoeld om de algemene arbeidsverhouding tussen een verwerkingsverantwoordelijke of verwerker en diens personeelsleden te regelen.

Afgezien van de specifieke bescherming van de functionaris voor gegevensbescherming waarin artikel 38, lid 3, tweede volzin, van de richtlijn gegevensbescherming voorziet, valt de vaststelling van regels inzake de bescherming tegen ontslag van een functionaris voor gegevensbescherming die in dienst is van een verwerkingsverantwoordelijke of verwerker, niet binnen de werkingssfeer van de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens, noch binnen de werkingssfeer van het vrije verkeer van die gegevens, maar binnen de werkingssfeer van de sociale politiek.

Volgens artikel 4, lid 2, onder b), VWEU hebben de Unie en de lidstaten een gedeelde bevoegdheid op het gebied van sociaal beleid.

Het staat elke lidstaat vrij specifieke bepalingen vast te stellen die meer bescherming bieden met betrekking tot het ontslag van de functionaris voor gegevensbescherming, mits die bepalingen verenigbaar zijn met het recht van de Unie en de bepalingen van de GDPR.

Een dergelijke verhoogde bescherming mag de verwezenlijking van de doelstellingen van de GDPR niet in gevaar brengen. Dit zou het geval zijn indien het in de weg stond aan het ontslag van een functionaris voor gegevensbescherming die niet langer de vereiste professionele kwaliteiten bezat om zijn taken uit te voeren of die deze taken niet overeenkomstig de bepalingen van de GDPR uitvoerde.

Het Hof concludeert dat artikel 38, lid 3, tweede volzin, van de richtlijn zich niet verzet tegen een nationale regeling die bepaalt dat een verwerkingsverantwoordelijke of een verwerker een functionaris voor gegevensbescherming die deel uitmaakt van zijn personeel, slechts om ernstige redenen kan ontslaan, zelfs indien het ontslag geen verband houdt met de uitoefening van zijn functie, mits een dergelijke regeling de verwezenlijking van de doelstellingen van de richtlijn niet in gevaar brengt.

12. Persoonsgegevens. Definitie

Wat zegt de Autoriteit Persoonsgegevens over persoonsgegevens?
Zie https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/mag-u-persoonsgegevens-verwerken

Wat zegt de rijksoverheid over persoonsgegevens?
https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/vraag-en-antwoord/mogen-organisaties-mijn-persoonsgegevens-aan-anderen-doorgeven

Wat valt er onder persoonsgegevens?
Onder persoonsgegevens vallen natuurlijk namen, adressen, telefoonnummers en e-mailadressen. De KvK-gegevens van eenmanszaken en VOF's zijn meestal ook persoonsgegevens. Een zakelijk persoonlijk doorkiesnummer en zakelijk persoonlijk e-mailadres zijn ook persoonsgegevens.

Wat valt er niet onder persoonsgegevens?
Alleen gegevens voor persoonlijke gebruik – denk aan de gegevens in je telefoonboekje, de verjaardagskalender, telefoonnummers in je telefoon en WhatsApp-groepen, en in persoonlijke notities – vallen niet onder de AVG.
Gegevens van organisaties, bijvoorbeeld een zakelijk telefoonnummer, vallen niet onder de AVG.

Wat zijn bijzondere en gevoelige persoonsgegevens?
Burgerservicenummer, geloofsovertuiging, seksuele voorkeur, ras en medische of biometrische gegevens en nog meer van dat soort informatie. Deze mogen minder snel verzameld worden dan de algemene persoonsgegevens.

Wat wordt verstaan onder de verwerking van persoonsgegevens?
Onder het verwerken van persoonsgegevens valt ongeveer ieder werkwoord, zoals: kopiëren, verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of een andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen en het afschermen, uitwissen of vernietigen van gegevens.

Mag een werkgever persoonsgegevens als een bankrekeningnummer verwerken?
Een werkgever mag het bankrekening nummer registreren want er moet immers uitvoering aan een arbeidsovereenkomst gegeven worden. Het loon moet aan een werknemer kunnen worden uitbetaald.

Heeft MAAS een uitgebreider document waarin dit alles gedetailleerd beschreven staat?
Ja, in het document *Informatiebeveiligingsbeleid MAAS i*s beschreven welke maatregelen MAAS neemt tegen oneigenlijk gebruik van gegevens en kunt u vinden wat er gebeurt mocht er een gegevenslek ontstaan. Dit document wordt standaard aan de Verwerkersovereenkomst toegevoegd. Als u meer wilt weten kunt u uiteraard contact met ons opnemen.

Is een gebruikersnaam een persoonsgegeven?
De gebruikersnaam is meestal een unieke naam zoals de eigen naam van de gebruiker, zijn/haar e-mailadres, of een pseudoniem/nickname. Een gebruikersnaam dient per definitie voor de identificatie van een natuurlijk persoon. We kunnen daarbij dus kort zijn: een gebruikersnaam (pseudoniem of niet) is een persoonsgegeven.

Is een (gehasht) wachtwoord een persoonsgegeven?
Het wachtwoord (of password) betreft een geheime reeks aan tekens, gekoppeld aan de gebruikersnaam, waardoor degene die de combinatie kent toegang verschaft tot de online service. Dat wachtwoord is echter niet bekend bij de online dienstverlener, maar wordt door haar enkel in een gehashte vorm opgeslagen. Kan een persoon dan nog wel geïdentificeerd worden aan de hand van het gehashte bestand alleen?
Een gehasht wachtwoord betreft een opgeslagen versie van een wachtwoord dat niet te herleiden is tot het oorspronkelijke wachtwoord: er wordt namelijk gebruik gemaakt van een onomkeerbaar algoritme. Daardoor kan uit het wachtwoord wel de gehasthe vorm worden berekend (en worden gecontroleerd), maar uit de gehashte vorm niet het wachtwoord (en worden herleid).
Zelfs al zou je het algoritme kennen waarmee de wachtwoorden worden gehasht, dan nog weet je niet wat het wachtwoord is. Je kan met de gehasthe vorm van een wachtwoord dus geen persoon identificeren. Het bij de online dienstverlener opgeslagen gehashte wachtwoord betreft dus geen persoonsgegeven.
Het wachtwoord zelf – dus de niet-gehasthe reeks aan tekens die de gebruiker invoert om te kunnen inloggen – kan wel als persoonsgegeven worden gezien. Het wachtwoord is immers juist bedoeld om, in combinatie met de gebruikersnaam, de gebruiker te identificeren. Daarbij maakt het niet uit of het wachtwoord zo simpel is als bijvoorbeeld de geboortedatum van de gebruiker (en dus an sich al direct een persoon zou kunnen identificeren), of een onleesbare reeks als @8vnv))32$V1 (en daarmee enkel in combinatie met de gebruikersnaam een persoon kan identificeren).

Is er sprake van verwerking van persoonsgegevens?
Zowel het invoeren van een wachtwoord, het controleren van het wachtwoord, als het hashen van een wachtwoord betreft dus een verwerking van persoonsgegevens. Van belang is wel dat er enige feitelijke macht moet kunnen worden uitgevoerd over die gegevens. Dat is het geval bij voornoemde handelingen: door middel van een volledig automatische procedure wordt het ingevoerde wachtwoord afgeschermd, gecontroleerd en gehasht. DE AVG is dus van toepassing op een inlogprocedure met gebruikersnaam en wachtwoord. In principe ben je dus onder meer verplicht om een privacy verklaring te hanteren, waarin de gebruiker wordt uitgelegd dat zijn/haar gebruikersnaam en wachtwoord worden verwerkt met als doel om te beoordelen of de gebruiker daadwerkelijk degene is die hij zegt dat hij is (authenticatie). Ook zal de gebruiker moeten worden geïnformeerd dat het wachtwoord in gehashte vorm wordt opgeslagen, zodat deze adequaat beveiligd is.

Zijn bedrijfsgegevens persoonsgegevens?
Activiteiten vallen sneller onder de privacywet, dan voorheen. Naast namen van personen en adressen vallen ook gegevens gekoppeld aan IP-adressen, cookies, een e-mailadres en dergelijke onder de wet. Ook als je niet weet wie er schuilgaat achter deze gegevens, moet je ze als privacygevoelig behandelen.
Je hebt al met de AVG te maken door het uitsturen van een offerte, factuur of (digitale) nieuwsbrief. Of door het bijhouden van afspraken met klanten, contactgegevens van klanten (zoals adres, e-mailadres of telefoonnummers) of personeelsinformatie.

Wat zijn directe en indirecte identificatoren?
AVG breidt uit op criteria met betrekking tot het identificeren van personen en bevat specifiek 'locatiegegevens' en 'een online identificator '-informatie. Directe en indirecte identificatoren: In tegenstelling tot de oude richtlijn is in AVG vastgelegd wat onder persoonsgegevens wordt verstaan hier worden specifiek de criteria 'locatiegegevens' en 'een online identificatoren' aan toegevoegd. Hieronder vallen onder andere:

- Connected devices; laptops, tablets, mobiele telefoon
- Applicaties, tools en protocollen; IP-adressen (Internet Protocol), identificatie cookies
- En andere zoals; Radio Frequentie Identificatie (RFID) tags
- Wat ons uiteindelijk brengt bij IOT (Internet of Things).

Wat zijn persoonsgegevens?
Als je gaat ondernemen krijg je met ontzettend veel dingen te maken waarmee je als individu niet, niet zo snel, of niet op dezelfde manier te maken krijgt. Een van die dingen is de Algemene verordening gegevensbescherming (AVG). Waar je als individu over het algemeen kunt profiteren van de zogenaamde huishoudelijke exceptie (als je al persoonsgegevens verwerkt, verwerk je die voor niet-zakelijke doeleinden) waardoor de AVG niet van toepassing is, zal de AVG al snel van toepassing zijn op de verwerkingsactiviteiten die je als ondernemer uitvoert. Om die reden is het van groot belang als (startende) ondernemer goed duidelijk te hebben welke persoonsgegevens je verwerkt, zodat je ervoor kunt zorgen dat je die persoonsgegevens verwerkt op een manier die door de AVG is toegestaan. Daarnaast kleeft er nóg een groot voordeel aan het helder hebben van welke persoonsgegevens je verwerkt. In de praktijk zien wij namelijk vaak dat van bepaalde gegevens wordt aangenomen dat het persoonsgegevens zijn, terwijl dat helemaal niet het geval is. Die gegevens mogen dan eigenlijk veel vrijer, bijvoorbeeld voor meer doeleinden, gebruikt worden dan gedacht. Om die gegevens volledig te kunnen benutten, is het erg belangrijk om goed te onderscheiden welke gegevens wél en welke gegevens níét kwalificeren als persoonsgegevens. In het vervolg van dit blog zal worden ingegaan op de vraag welke gegevens kwalificeren als persoonsgegevens en worden handvaten gegeven om dit begrip in de praktijk toe te passen.

Wat zijn persoonsgegevens volgens de AVG?
De AVG geeft in artikel 4 een definitie van het begrip "persoonsgegevens". Volgens de AVG is een persoonsgegeven "alle informatie over een geïdentificeerde of identificeerbare natuurlijk persoon". Uit deze definitie volgen twee voorwaarden waaraan informatie moet voldoen om te kwalificeren als persoonsgegeven, namelijk:

- De informatie moet betrekking hebben op een natuurlijke persoon; en
- Die natuurlijke persoon moet geïdentificeerd of identificeerbaar zijn.

Aan de eerste voorwaarde is voldaan als gegevens iets zeggen over een bepaalde natuurlijke persoon. Hierbij moet worden bedacht dat gegevens al vrij snel iets zeggen over een bepaalde natuurlijke persoon. Zo is een huisnummer een (erg concrete) indicator van de plaats waar iemand woont. Naast dat een huisnummer iets zegt over een persoon (namelijk waar diegene woont), is het ook mogelijk om (mede) aan de hand van een huisnummer een persoon te identificeren. Met alleen een huisnummer is dit uiteraard lastig (immers, dit is niet meer dan een cijfer), maar wanneer je weet dat je een man of vrouw zoekt die in een bepaalde straat woont, maakt het huisnummer het in veel gevallen mogelijk die persoon te identificeren. Het huisnummer maakt het daardoor in vrijwel alle gevallen (potentieel) mogelijk een natuurlijke persoon te identificeren. Om die reden is een huisnummer in de regel dan ook een persoonsgegeven.

Wat is pseudonimiseren?
In veel gevallen zijn persoonsgegevens alleen nuttig als je deze kunt koppelen aan degene waarvan de persoonsgegevens afkomstig zijn. Bijvoorbeeld wanneer een klant een bestelling heeft geplaatst en je het huisnummer nodig hebt om de bestelling op de juiste plek af te kunnen leveren. Bij de verwerking van het huisnummer moet dus rekening worden gehouden met de regels die de AVG geeft. Een van die regels is dat je de privacy van degenen waarvan de persoonsgegevens afkomstig zijn moet beschermen. Een manier om dit te doen is het pseudonimiseren van de gegevens. Gepseudonimiseerde gegevens zij nog wel te herleiden naar een persoon, maar dit is wel lastiger gemaakt. Zo kun je bijvoorbeeld in plaats van de naam van de klant, de bestelling een bepaalde code geven. Het huisnummer wordt dan aan een code gekoppeld in plaats van aan een persoon, waardoor de gegevens minder bruikbaar zijn voor kwaadwillende derden.

Wat is anonimiseren?
Daarnaast kun je de persoonsgegevens anonimiseren. Wanneer je persoonsgegevens anonimiseert, zorg je ervoor dat deze niet meer tot een persoon herleidbaar zijn. Geanonimiseerde gegevens zijn derhalve geen persoonsgegevens meer en de AVG is dan ook niet meer van toepassing op de verwerking van deze gegevens. Dit is bijvoorbeeld mogelijk wanneer je bijvoorbeeld een onderzoek zou willen doen naar de huisnummers van jouw klanten, om in kaart te brengen op welke huisnummers jouw klanten wonen. Je kunt dan enkel en alleen de huisnummers noteren, waardoor je slechts de cijfers overhoudt. Deze zijn dan niet meer herleidbaar tot natuurlijke personen, maar geven wel inzicht in op welke huisnummers jouw klanten wonen. Dit is wellicht een flauw voorbeeld van de mogelijkheid om te anonimiseren omdat dit onderzoek waarschijnlijk geen nuttige inzichten zal geven. Echter, voor de resultaten van veel onderzoeken geldt dat door input volledig los te koppelen van personen, anonieme gegevens kunnen worden gecreëerd. Als dit is gedaan, is geen sprake meer van persoonsgegevens waardoor de AVG geen toepassing meer vindt. De gegevens zijn daardoor veel breder bruikbaar geworden.

Bron:
https://ploum.nl/nieuws/wat-zijn-persoonsgegevens

13. Persoonsgegevens. Uitwisselen

Wat zegt de Autoriteit Persoonsgegevens over persoonsgegevens uitwisselen?
https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/verstrekken-van-persoonsgegevens

Ander bronnen over persoonsgegevens uitwisselen:
https://www.dirkzwager.nl/kennis/artikelen/de-verschillende-soorten-afspraken-bij-de-uitwisseling-van-persoonsgegevens/

Welke situaties bij uitwisselen van persoonsgegevens?

1. uitbesteden;
2. doorgeven;
3. samenwerken.

Wat is (volledig) uitbesteden?
Het komt heel vaak voor dat bedrijfsprocessen worden uitbesteed. Denk aan het afnemen van IT-diensten vanuit de cloud (in plaats van een eigen IT-afdeling) of het gebruik van een externe salarisadministratie. Vaak behoort het verwerken van persoonsgegevens tot de kern van deze uitbestede werkzaamheden. Je kunt immers geen IT-systeem in de lucht houden zonder gebruikersnamen en je kunt geen salaris verwerken zonder gegevens over die werknemers te ontvangen. In degelijke situaties kwalificeert die leverancier volgens de privacywetgeving als "verwerker". Het is in die gevallen wettelijk verplicht een verwerkingsovereenkomst te sluiten. Dat staat in artikel 28 van de Algemene Verordening Gegevensbescherming (AVG). De AVG schrijft ook dwingend voor welke onderwerpen in zo'n overeenkomst aan de orde moeten komen. De vorm is echter vrij; de wet schrijft niet een modelcontract voor. Vooraf moet je toetsen of de leverancier wel betrouwbaar is en gedurende de looptijd van de overeenkomst moet je toezien dat deze de persoonsgegevens zorgvuldig verwerkt.
Kenmerkend aan de rol van verwerker is dat deze de persoonsgegevens absoluut niet voor eigen doeleinden mag gebruiken.

Wat is doorgeven?
De ontvangende partij verwerkt bij doorgeven de gegevens verder voor eigen doeleinden. Denk hierbij aan:

- het doorgeven van gegevens van werknemers door een werkgever aan een pensioenfonds of een leasemaatschappij;
- het doorgeven van gegevens door een medicus aan een opvolgend behandelaar;
- het doorgeven van adresgegevens aan een bezorgservice;
- het doorgeven van adresgegevens aan een onderhoudsbedrijf

In al deze situaties moet aan de hand van de privacywetgeving worden getoetst of doorgifte is toegestaan. Dat betekent dat o.a. moet worden nagedacht over:

- proportionaliteit en subsidiariteit: is de doorgifte noodzakelijk, worden niet teveel gegevens doorgegeven
- grondslag: ligt de doorgifte dicht bij de verwachting van betrokkene, is deze wettelijk verplicht of is wellicht toestemming nodig?
- doelbinding: past de doorgifte bij de redenen waarvoor de gegevens zijn verkregen
- transparantie: weet de betrokkene van de doorgifte of kan hij deze verwachten
- beveiliging: is de doorgifte goed beveiligd

- bij bijzondere persoonsgegevens: is de doorgifte wettelijk toegestaan of is er toestemming van de betrokkene

In een overeenkomst staan afspraken worden gemaakt over o.a. transparantie (wie informeert: verstrekker of ontvanger?), beveiliging (hoe vindt veilige uitwisseling plaats?) en de ketenverplichtingen bij uitoefenen van rechten van betrokkenen (met name doorgeven van correctieverzoeken). Ook afspraken over aansprakelijkheid, voor het geval geclaimd wordt dat de doorgifte niet rechtmatig zou zijn.
Kenmerkend aan doorgifte is dat de ontvangende partij, behoudens andere afspraken, in principe vrij is de persoonsgegevens verder te verwerken (binnen wettelijke kaders). Dit verschilt dus sterk van de verwerkerssituatie. In deze situatie moet ook absoluut geen verwerkersovereenkomst worden getekend!

Wat is samenwerken?
In artikel 26 AVG is bepaald dat de samenwerkende partijen een regeling moeten vaststellen. In die regeling moet de verdeling van verantwoordelijkheden duidelijk worden vastgelegd, met name in relatie tot de betrokkene. De kern van die regeling moet aan de betrokkene kenbaar worden gemaakt.

Er moet dus in deze situatie een overeenkomst zijn. Naast de verdeling van verantwoordelijkheden (zie hiervoor), is het ook verstandig afspraken te maken hoe overigens samen te voldoen aan de privacywetgeving. Partijen voeren immers een gezamenlijke administratie en zij kunnen daar hoofdelijk op worden aangesproken. Verder zal er een duidelijke exit-regeling moeten zijn, waaruit volgt of (de gegevens uit) die gezamenlijke administratie ook na de samenwerking nog door partijen mogen worden gebruikt.

Bron: https://www.awvn.nl/privacy-arbeidsrelatie-personeelsgegevens-en-instanties-en-landen/

Wanneer mag ik zonder toestemming van de medewerker gegevens verstrekken aan andere instanties?
Dit mag zonder toestemming als dit noodzakelijk is voor de uitvoering van het arbeidscontract of om aan een wettelijke verplichting te kunnen voldoen. Denk aan de leasemaatschappij of het UWV als de medewerker wordt ziek gemeld.

Mag ik persoonsgegevens van een medewerker geven aan de politie als die daarom vraagt?
U bent alleen verplicht gegevens te verstrekken als de politie hier gericht om vraagt en aangeeft op grond van welke wettelijke regeling dat gevraagd wordt. Bijvoorbeeld op bevel van een rechter-commissaris of om bepaalde misdrijven op te lossen.

Mag ik persoonsgegevens van een medewerker aan de deurwaarder geven als er sprake is van een loonbeslag?
De regel is dat de kring met personen die van het loonbeslag af weet, zo klein mogelijk wordt gehouden. U mag de leidinggevende en HR-medewerkers informeren, maar er geldt wel een geheimhoudingsplicht. U dient hen hierop te wijzen. De gegevens mogen voor geen andere doel worden gebruikt dan waarvoor ze verkregen zijn, namelijk de correcte afwikkeling van het loonbeslag.

Mag ik de leidinggevende van de medewerker informeren over een loonbeslag?
De regel is dat de kring met personen die van het loonbeslag af weet, zo klein mogelijk wordt gehouden. U mag de leidinggevende en HR-medewerkers informeren, maar er geldt wel een geheimhoudingsplicht. U dient hen hierop te wijzen. De gegevens mogen voor geen andere doel

worden gebruikt dat waarvoor ze verkregen zijn, namelijk de correcte afwikkeling van het loonbeslag.

Mag ik persoonsgegevens van medewerkers naar andere EU landen sturen?
Ja, dat mag. Binnen de EU is het niveau van gegevensbescherming gelijk. Dat komt omdat alle EU lidstaten zich moeten houden aan de Algemene verordening gegevensbescherming (AVG). De EU is daarom één rechtsgebied ten aanzien van de bescherming van persoonsgegevens.
Geeft een organisatie gegevens door van Nederland naar een ander EU-land? Dan hoeft die organisatie alleen te voldoen aan de algemene eisen uit de AVG.

En als ik de persoonsgegevens naar landen buiten de EU wil sturen, zogenaamde derde landen?
Derde landen zijn alle landen buiten de EU, met uitzondering van Noorwegen, Liechtenstein en IJsland. Deze drie landen kennen een gelijkwaardig niveau van bescherming van persoonsgegevens. Hoofdregel is dat persoonsgegeven alleen aan derde landen mogen worden doorgegeven die een passend beschermingsniveau hebben. Als er geen sprake is van een derde land met een passend beschermingsniveau, is doorgifte slechts toegestaan op grond van een van de wettelijke bepalingen uit de AVG (hoofdstuk V). Op de site van de Autoriteit Persoonsgegevens vindt u een lijst met landen waar een passend niveau van bescherming aanwezig wordt geacht.

Hoe zit het beschermingsniveau in de Verenigde Staten?
In de Verenigde Staten (VS) bestaat geen algemene wetgeving voor de bescherming van persoonsgegevens. De VS hebben daarom geen passend beschermingsniveau. Dat betekent dat u niet zonder meer persoonsgegevens mag doorgeven aan de VS.

14. Persoonsgegevens. Publicatie personeelsgegevens

Wat zegt de AP over publicatie personeelsgegevens?
Niet specifiek over personeelsgegevens:

- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-en-uitkering
- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/foto-en-film/beeldmateriaal?qa=publicatie

Bron: https://www.awvn.nl/privacy-arbeidsrelatie-publicatie-personeelsgegevens/

Mag ik alle medewerkers met hun foto op onze website zetten?
Toestemming van de medewerker is nodig. Toestemming moet zowel voor het plaatsen van de foto als voor het noemen van de naam gegeven worden. Een werknemer moet op ondubbelzinnige wijze toestemming hebben gegeven voor het laten plaatsen van foto's op de website. Dit betekent dat de werknemer precies moet weten waar toestemming voor wordt gevraagd en wat het doel is. Ook moet de werkgever kunnen aantonen dat de werknemer toestemming heeft gegeven voor deze specifieke kwestie. Daarnaast moet de werkgever de werknemer mededelen dat hij zijn toestemming op ieder moment weer kan intrekken.

Mogen naam en foto van een medewerker op intranet worden geplaatst?
Ja, als het een strikt interne publicatie betreft, is het mogelijk dat het belang van de organisatie in plaats komt van de grond "toestemming" van de werknemer voor het plaatsen van de naam en foto van de werknemer. Hierbij is wel een afweging tussen het bedrijfsbelang en de privacy van de werknemer vereist.

Mag ik productiecijfers per medewerker op het intranet of prikbord publiceren?
Nee, dat mag niet op basis van de privacywetgeving. Productiecijfers kunnen onder meer iets zeggen over de gezondheid van een medewerker en die gegevens dienen extra beschermd te worden.

Mogen wij per team de behaalde resultaten per werknemer intern publiceren (papier en intranet)?
Dit betreft persoonsgegevens die vallen onder de bescherming van de AVG. Als de gegevens niet tot een individuele medewerker te herleiden zijn, mag het, anders niet.

Het publiceren van ongevalslijsten met vermelding van soort ongeval, letsel en naam medewerker, mag dat?
Nee, dit betreft persoonsgegevens die vallen onder de bescherming van de AVG. Het gaat hier ook nog eens om bijzondere persoonsgegevens, namelijk gegevens over de gezondheid van medewerkers. Daarvoor gelden extra strenge eisen.

Welk risico neem ik bij publicatie van persoonsgegevens of beelden van personen waarvoor geen toestemming van de betrokkene is?
Als organisatie handelt u onrechtmatig en overtreedt u mogelijk de Algemene Verordening Gegevensbescherming. Dit kan ertoe leiden dat de Autoriteit Persoonsgegevens bij u een controle komt uitvoeren. De Autoriteit Persoonsgegevens kan u ook een boete opleggen. Uw organisatie kan in sommige situaties ook verplicht worden tot het betalen van schadevergoeding.

15. Persoonsgegevens. Social media

Wat zegt de AP zelf over social media?
https://autoriteitpersoonsgegevens.nl/nl/nieuws/avg-guidelines-over-targeting-sociale-media-en-over-geschillen-edpb

Bron: https://www.awvn.nl/privacy-arbeidsrelatie-sociale-media-e-mail-internet/

Mijn medewerker twittert dat hij geen bonus krijgt, omdat ons bedrijf te weinig winst heeft gemaakt. Mag dat?
In verband met de privacy van uw organisatie (bedrijfsgevoelige informatie) handelt uw medewerker onrechtmatig en kunt u hem hierop aanspreken. Voor het gebruik van sociale media in relatie tot de bescherming van de belangen van uw organisatie kunt u gedragsregels opstellen.
Sociale media zijn niet meer weg te denken uit onze maatschappij. Net zo min als internet en e-mail. Digitale ontwikkelingen volgen elkaar in rap tempo op. Bedrijven kunnen er niet meer om heen, maar moeten er wel verstandig mee omgaan. AWVN adviseert werkgevers daarom transparant beleid te voeren ten aanzien van het gebruik van sociale media en internet – om zo de positieve effecten van het gebruik te benutten en de mogelijk negatieve effecten tot een minimum te beperken.

Hoe stuur ik het gebruik van sociale media vanaf de werkplek?
U kunt het beste hierover een gedragscode opstellen. Neem daarin ook een paragraaf over tijdsbesteding op.

Heeft de ondernemingsraad instemmingsrecht bij invoering voor een gedragscode met betrekking tot het gebruik van sociale media?
Ja, de ondernemingsraad heeft instemmingsrecht op grond van artikel 27 lid 1 sub k en l van de Wet op de ondernemingsraden. De instemming van de ondernemingsraad is in het bijzonder vereist, indien in het social-media-protocol een regeling is opgenomen voor het monitoren door de werkgever van het gebruik van social media door werknemers. Ook moet u al het personeel informeren bij invoering.

Mag ik op geregelde basis het e-mail en internetgebruik van medewerkers controleren?
U mag voorwaarden stellen aan het gebruik van e-mail en internet op het werk of bepaalde soorten gebruik verbieden. Vervolgens mag u controles uitvoeren. U moet daarbij wel voldoen aan de voorwaarden uit onder meer de Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG). Het controleren van het e-mail- en internetgebruik van medewerkers is aan te merken als een personeelsvolgsysteem.

Mag ik alle e-mails van mijn medewerkers uitgebreid controleren?
Nee, er mag slechts beperkt worden gecontroleerd. Bij controle van e-mailberichten dient de inhoud van privé e-mailberichten ontzien te worden. Er moet onderscheid worden gemaakt tussen zakelijke en privé e-mail. Het is nog beter om maatwerk uit te voeren door controles te beperken tot louter verdachte medewerkers. Informatie in e-mailverkeer van medewerkers met een beroepsgeheim, zoals leden van de ondernemingsraad en bedrijfsartsen, moet volledig worden ontzien.

Wat hanteer ik als doel van een e-mailcontrole?
Het doel van de controle op e-mail en internetgebruik is doorgaans de controle op naleving van de hierover in de organisatie opgestelde richtlijn. Een doel kan bijvoorbeeld ook zijn: systeem- en

netwerkbeveiliging, beschermen van bedrijfsgeheimen of verminderen van kosten en tijdsverlies. Denk ook aan een verbod op bezoek van bepaalde websites die de goede naam van uw organisatie zouden kunnen aantasten (porno/kansspelen). U kunt bezoek aan deze verboden websites blokkeren, zodat bezoek door medewerkers niet mogelijk is.

Heeft de ondernemingsraad instemmingsrecht bij invoering van een controlesysteem?
Ja, bij invoering, wijziging of intrekking van een controlesysteem/richtlijn heeft de ondernemingsraad instemmingsrecht.

Hoe informeer ik mijn medewerkers over een richtlijn over gebruik e-mail en internet en de controle daarvan?
Voor de gebondenheid door de medewerkers aan de richtlijn kunt u het beste bij indiensttreding de medewerker de richtlijn laten ondertekenen. En in de arbeidsovereenkomst kunt u vermelden dat de richtlijn een integraal onderdeel is van de arbeidsverhouding. Voor de gebondenheid is niet voldoende dat de ondernemingsraad heeft ingestemd met de richtlijn.

16. Persoonsgegevens. Bijzondere en strafrechtelijke

Wat zegt de Autoriteit Persoonsgegevens over bijzondere persoonsgegevens?
Zie https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/mag-u-persoonsgegevens-verwerken

Jurisprudentie:

- https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2009:BH4720
- https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2018:3354

Wat ziet de AP als bijzondere persoonsgegevens?
De AVG ziet deze persoonsgegevens als bijzondere persoonsgegevens:

1. Persoonsgegevens waaruit ras of etnische afkomst blijkt;
2. Persoonsgegevens waaruit politieke opvattingen blijken;
3. Persoonsgegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken;
4. Persoonsgegevens waaruit het lidmaatschap van een vakvereniging blijkt;
5. Gegevens over gezondheid;
6. Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid;
7. Genetische gegevens;
8. Biometrische gegevens met het oog op de unieke identificatie van een persoon.

Wat ziet de AP als strafrechtelijke persoonsgegevens?
Strafrechtelijke persoonsgegevens zijn persoonsgegevens die te maken hebben met strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen. Hieronder vallen zowel veroordelingen als mogelijk gegronde verdenkingen. Dit wil zeggen dat er concrete aanwijzingen zijn dat iemand een strafbaar feit heeft gepleegd. Een voorbeeld hiervan is een opgestelde zwarte lijst van frauderende klanten bij een financiële instelling.
Met ‘veiligheidsmaatregelen’ worden persoonsgegevens bedoeld die te maken hebben met een door de rechter opgelegd verbod voor onrechtmatig of hinderlijk gedrag.

Wat ziet de Hoge Raad als strafrechtelijke persoonsgegevens?
Onder 'strafrechtelijke persoonsgegevens' zijn te verstaan “…zodanige concrete feiten en omstandigheden dat zij een als strafbaar feit te kwalificeren bewezenverklaring - in de zin van art. 350 Sv. - kunnen dragen" en in dat verband - evenzeer terecht - als maatstaf genomen of de vastgestelde gedragingen een zwaardere verdenking dan een redelijk vermoeden van schuld opleveren, in die zin dat de te verwerken strafrechtelijke persoonsgegevens in voldoende mate moeten vaststaan.
Slechts een redelijk vermoeden van schuld (de standaard om aangifte te kunnen doen of vervolging te starten) is onvoldoende om te spreken van strafrechtelijke persoonsgegevens.
Uit het voorgaande vloeit voort dat niet snel mag worden aangenomen dat verwerkte gegevens strafrechtelijke persoonsgegevens zijn. Niet voldoende is dat de betrokkene wordt beschuldigd van strafbaar gedrag. De wetsgeschiedenis en jurisprudentie bieden voldoende aanwijzingen dat het moet gaan om bewezen feiten, of gegronde verdenkingen, dus verdenkingen die zijn onderbouwd met concrete, voldoende zwaarwegende aanwijzingen dat een bepaald persoon zich aan strafbaar gedrag heeft schuldig gemaakt.

17. Grondslagen. Proportionaliteit en subsidiariteit

Wat zegt de AP over proportionaliteit en subsidiariteit?
Geen actuele info?

Beginselen van proportionaliteit en subsidiariteit?
De Hoge Raad heeft in zijn beschikking van 9 september 2011 benadrukt dat bij iedere verwerking van persoonsgegevens voldaan moet zijn aan de beginselen van proportionaliteit en subsidiariteit. De verantwoordelijke moet, op basis van de bij hem bekende gegevens, steeds een belangenafweging maken tussen het eigen belang en dat van de betrokkene.
https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2011:BQ8097&showbutton=true
Deze belangrijke beginselen zijn relevant voor de beoordeling van elke verwerking van persoonsgegevens, die op een andere grondslag worden verwerkt dan met toestemming van de betrokkene. Wanneer je persoonsgegevens verwerkt op basis van één van de 'noodzakelijkheidsgrondslagen', zal u zich telkens dienen af te vragen of de verwerking proportioneel is en of de verwerking voldoet aan de eis van subsidiariteit. Vuistregels daarbij zijn voor het bewaren 'hoe korter, hoe beter' en voor de toegankelijkheid 'hoe minder, hoe beter'.

Staat het doel van de verwerking in verhouding tot de inbreuk voor de personen van wie u persoonsgegevens verwerkt?
Het proportionaliteitsvereiste brengt met zich dat het doel van de verwerking van de persoonsgegevens in verhouding moet staat tot de inbreuk op de privacy van de betrokkene. Dit betekent ook dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk. In dat kader is het van belang dat u een dataretentiebeleid opstelt, waaruit blijkt hoe lang u de verschillende persoonsgegevens bewaard. Sommige bewaartermijn volgen uit de wet, bijvoorbeeld op grond van belastingwetgeving. Hieruit volgt onder meer dat een werkgever een loonbelastingverklaring en een kopie van het identiteitsbewijs moet bewaren tot vijf jaar nadat de werknemer uit dienst is getreden. Voor bepaalde persoonsgegevens bestaan er richtlijnen zoals:

- een bewaartermijn van twee jaar na uitdiensttreding voor het personeelsdossier; en
- een bewaartermijn van vier weken na het einde van de sollicitatieprocedure voor sollicitatiegegevens.

Daarnaast mogen persoonsgegevens alleen toegankelijk zijn voor diegene die kennis moeten nemen van de informatie. Hiervoor is een autorisatiebeleid van belang waaruit volgt wie er toegang mogen hebben tot bepaalde persoonsgegevens. Hieruit kan onder meer volgen dat:

- de toegang tot salarisgegevens beperkt is tot die personen die belast zijn met de salarisadministratie;
- het personeelsdossier alleen kan worden ingezien door HR-medewerkers en de direct leidinggevende; en
- klantgegevens slechts toegankelijk zijn voor de commerciële afdeling.

Daarnaast moet de verwerking effectief zijn. Als met de verwerking van de gegevens niet het gestelde doel kan worden bereikt, dan is de verwerking niet proportioneel.

Kan het doel ook op een andere wijze worden bereikt waarbij de inbreuk op de privacy van de betrokkene minder is?
Op basis van het subsidiariteitsvereiste moet altijd gekeken worden of het beoogde doel dat voor de verwerking is vastgesteld, ook op een minder ingrijpende manier en / of met minder ingrijpende middelen kan worden bereikt. De gedachte hierachter is dat bij de verwerking van persoonsgegevens de privacy van de betrokkene en eventuele derden, zo min mogelijk geschaad mag worden.

18. Grondslagen. Voor verwerking van persoonsgegevens

Wat zegt de Autoriteit Persoonsgegevens over grondslagen?
Zie: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/mag-u-persoonsgegevens-verwerken

Wat zijn grondslagen?
Om een zorgvuldige verwerking van persoonsgegevens te waarborgen, staat in de AVG dat persoonsgegevens alleen mogen worden verwerkt voor zover daarvoor een grondslag aanwezig is. De wet vermeldt zes mogelijke grondslagen. De zes grondslagen zijn:

1. toestemming van de betrokkene; en/of
2. noodzakelijk voor precontractuele maatregelen of uitvoering overeenkomst; en/of
3. noodzakelijk voor nakoming wettelijke verplichting; en/of
4. noodzakelijk ter vrijwaring vitaal belang betrokkene; en/of
5. noodzakelijk voor uitvoering publieke taak; en/of
6. noodzakelijk voor behartiging gerechtvaardigd belang.

Wat zijn de meest bruikbare grondslagen?
Zolang er niet meer gegevens worden verwerkt dan noodzakelijk, zijn in de praktijk voor commerciële organisaties de meeste verwerkingen prima te scharen onder de grondslagen "uitvoering overeenkomst", "wettelijke plicht" en "gerechtvaardigd belang". Voor publiekrechtelijke organisaties geldt dat de "uitvoering publieke taak" meer opspeelt en "gerechtvaardigd belang" niet of minder.

Zijn alleen grondslagen voldoende voor een zorgvuldige verwerking van persoonsgegevens?
Naast de grondslagen gelden - vanwege diezelfde zorgvuldigheid - ook andere eisen: doelbinding, beveiliging, geheimhouding.

Wat wordt bedoelt met doelbinding?
Met doelbinding wordt bedoeld dat de persoonsgegevens die je verwerkt heb gekregen voor een bepaald doel. Bijvoorbeeld een medewerker van een klant geeft je zijn adresgegevens voor het sturen van een offerte. Het is belangrijk dat je persoonsgegevens alleen verwerkt (dus opslaat en gebruikt) voor de doeleinden waarvoor je deze hebt verkregen.

Toetsing verwerking
De Hoge Raad plaatst de verwerking van persoonsgegevens in http://uitspraken.rechtspraak.nl/#zoekverfijn/ljn=BQ8097&so=Relevance uitdrukkelijk in het kader van artikel 8 EVRM. Dat is op zichzelf niet zo verrassend, want ook het Europese Hof van Justitie toetst verwerkingen van persoonsgegevens in het arrest Schecke & Eifert v. Hessen https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX:62009CJ0092 aan dit grondrecht. Toch leidt dit er wel toe dat de plicht tot zorgvuldige gegevensverwerking uit de AVG (informationele privacy), in de concrete uitwerking wat meer grondrechtelijke trekken krijgt (relationele privacy). Het onderscheid tussen beide privacy-begrippen vervaagt aldus.

19. Grondslag. Toestemming

Wat zegt de Autoriteit Persoonsgegevens over grondslagen toestemming?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken#wanneer-mag-u-zich-baseren-op-de-grondslag-toestemming-6331

Is toestemming een handige grondslag?
Toestemming vragen is vaak helemaal niet nodig, tenzij er meer gegevens worden verwerkt dan noodzakelijk of wanneer er bijzondere persoonsgegevens worden verwerkt. Van de zes grondslagen is toestemming de minst handige grondslag. Daarvoor zijn meerdere redenen:

- er worden zware eisen gesteld aan een toestemmingsverklaring, wil deze überhaupt geldig zijn;
- toestemming ziet altijd op een specifieke verwerking;
- toestemming vragen kan misleidend zijn;
- toestemming vragen leidt tot een zware administratieplicht;
- een gegeven toestemming kan altijd worden ingetrokken.

Wanneer is toestemming geldig?
Toestemming is binnen de AVG: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt

Wanneer is toestemming niet geldig?
Iedere toestemmingsverklaring of handeling waarvan achteraf kan worden gezegd dat deze

- niet in vrijheid is gegeven; en/of
- niet voldoende specifiek is; en/of
- niet op (juiste) informatie is berust; en/of
- onvoldoende ondubbelzinnig is in de aldus geuite wil;

Wat is een specifieke verwerking?
Een blanco volmacht kan nooit kwalificeren als geldige toestemming. Dat betekent dat een organisatie die leunt op het vragen van toestemming, voor iedere nieuwe verwerking van persoonsgegevens opnieuw toestemming zal moeten vragen.

Waarom kan toestemming vragen misleidend zijn?
Betrokkene heeft bij het geven van toestemming de indruk dat hij/zij controle heeft over wat er met de eigen persoonsgegevens gebeurt. Dat is echter bijna nooit volledig juist. Organisaties die persoonsgegevens verwerken hebben namelijk ook te maken met allerlei wettelijke verplichtingen, waardoor de persoonsgegevens weer doorgegeven moeten worden aan andere instanties. Een organisatie die voor iedere verwerking van persoonsgegevens om toestemming vraagt, wekt mogelijk de indruk dat dit niet het geval is. Dat roept vragen op over de geldigheid van de aldus verkregen toestemming.

Hoe voldoe je bij de toestemming aan de zware administratieplicht?
Wie zich beroept op toestemming, moet kunnen bewijzen dat er daadwerkelijk geldig toestemming is gegeven. Dat veronderstelt dus dat er een administratie van gegeven toestemming wordt opgezet. Die administratie dient op zijn beurt weer goed beveiligd en beheerd te zijn.

Wat betekent het intrekken van toestemming door betrokkene?
Zodra de toestemming wordt ingetrokken, stort ieder systeem waarbij persoonsgegevens worden verwerkt dat gebaseerd is op toestemming als een kaartenhuis in elkaar. Als het kaartenhuis op dat moment niet in elkaar stort - de verwerking gaat gewoon door - dan is ten onrechte toestemming gevraagd. De Autoriteit Persoonsgegevens kan dan handhavend optreden en forse boetes opleggen.

20. Grondslag. Uitvoering van een overeenkomst

Wat zegt de Autoriteit Persoonsgegevens over grondslag uitvoering van een overeenkomst:
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken#wanneer-mag-u-zich-baseren-op-de-grondslag-uitvoering-overeenkomst-6332

21. Grondslag. Nakomen van een wettelijke verplichting

Wat zegt de Autoriteit Persoonsgegevens over grondslag nakomen van een wettelijke verplichting
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken#wanneer-mag-u-zich-baseren-op-de-grondslag-wettelijke-verplichting-6333

Welke persoonsgegevens vastleggen ten aanzien van ongevallen en incidenten?
Wettelijke verplichtingen:
Een werkgever is op basis van artikel 9 van de Arbowet verplicht om alle arbeidsongevallen die tot meer dan drie dagen ziekteverzuim leiden, te registreren. De Preventiemedewerker legt deze informatie vast in het digitale meldingsformulier en archivering in een digitaal register. HR draagt zorg voor verdere afhandeling, zoals communicatie met leidinggevende en arbodienst.

Betrokkene en gegevens ten aanzien van ongevallen en incidenten. Van wie worden welke gegevens verwerkt en wat is het doel hiervan?
Persoonsgegevens:

- Gegevens: Naam + functie + organisatieonderdeel + omschrijving (bijna) ongeval + aard van het letsel + aantal verzuimdagen.
- Verzameldoel: Het doel van deze regeling is in eerste instantie dat deze gegevens goed kunnen worden geregistreerd en onderzocht, zodat maatregelen kunnen worden genomen om herhaling van de ongewenste gebeurtenis te voorkomen. Daarnaast kan door het melden van onveilige situaties zelfs al eerder worden voorkomen dat het mis gaat. Zodoende leveren meldingen een bijdrage aan verdere verbetering van de arbeidsomstandigheden. Ook wordt met deze regeling voldaan aan de verplichtingen in de Arbowet.
- Bewaartermijn: De persoonsgegevens worden bewaard overeenkomstig de wettelijke termijnen, die tot dertig jaar kunnen bedragen; de gebruikelijke verjaringstermijn in verband met persoonlijke rechtsvorderingen bedraagt echter tien jaar. Deze dossiers vallen onder archiefwet en zullen conform deze wet worden bewaard/vernietigd.
- Bron: Persoonsgegevens kunnen ook door leidinggevende of BHV-er worden aangeleverd m.b.t. een (bijna)ongeval. Daarnaast wordt een deel van de persoonsgegevens ontvangen na onderzoek en advies van bedrijfsartsen/ergonomen.
- Betrokkenen waren niet verplicht deze gegevens aan te leveren.

Bijzondere persoonsgegevens

- Gegevens over gezondheid

Automatische besluitvorming: Er is geen sprake van besluitvorming over persoonsgegevens op basis van automatisch verwerkte gegevens.

Ontvangers: Gegevens worden verstrekt aan onderstaande 'ontvangers'. Betreffende teammanager, Preventiemedewerker en bedrijfsarts ontvangen de persoonsgegevens. Iedere stakeholder ontvangt in het kader van dataminimalisatie alleen de gegevens die strikt noodzakelijk zijn.

Doorgifte buiten EU: Er is geen sprake van doorgifte van persoonsgegevens aan één of meer landen buiten de Europese Unie of aan een internationale organisatie

Vergelijk: https://www.avgregisterrijksoverheid.nl/verwerkingen/registratie-bijna-ongevallen

Welke persoonsgegevens vastleggen ten aanzien van gevaarlijke stoffen?
Wettelijke verplichtingen:

- Voldoen aan de wettelijke eisen uit het Arbobesluit. Hoofdstuk 4, specifieke artikel 4.2a (Nadere voorschriften risico inventarisatie en -evaluatie, aanvullende registratie), artikel 4.13 (Nadere voorschriften risico inventarisatie en –evaluatie) en artikel 4.15 (lijst van werknemers) Arbowet.
- Invulling zorgplicht MAAS vanuit goed werkgeverschap. Art. 7:611 BW

Betrokkene en gegevens bij gevaarlijke stoffen. Van wie worden welke gegevens verwerkt en wat is het doel hiervan?
Persoonsgegevens:

- Gegevens: Gewone persoonsgegevens - Arbeidsplaatsnummer en omschrijving - Naam (voorvoegsel, voornaam, achternaam) - Werknemer-ID - Zelf gedefinieerde functiegroep onder een bestaande afdeling -tot het niveau dat nodig is voor de betreffende afdeling waar de nadere inventarisatie Gevaarlijke Stoffen plaatsvindt
- Verzameldoel: Invulling zorgplicht MAAS vanuit goed werkgeverschap.
- Bewaartermijn:
    - 5 jaar: standaard RI&E onderzoeken & rapporten veiligheid/gezondheid conform Arbowet
    - 40 jaar: onderzoeken & rapporten veiligheid/gezondheid conform Arbowet. Betreft inventariseren, evalueren en beoordelen gevaren van arbeid waarbij werknemers aan kankerverwekkende stoffen of processen, lood, asbest, biologische agentia et cetera worden blootgesteld.
- Bron: HR-administratie
- Betrokkenen waren niet verplicht deze gegevens aan te leveren.

Bijzondere persoonsgegevens

- Gegevens over gezondheid

Automatische besluitvorming: Er is geen sprake van besluitvorming over persoonsgegevens op basis van automatisch verwerkte gegevens.

Ontvangers: Gegevens worden verstrekt aan onderstaande 'ontvangers'.

- Werkgever, afdelingshoofd en Preventiemedewerker
- Medewerkers die kunnen of worden blootgesteld aan gevaarlijke stoffen

Doorgifte buiten EU: Er is geen sprake van doorgifte van persoonsgegevens aan één of meer landen buiten de Europese Unie of aan een internationale organisatie.

Vergelijk: https://www.avgregisterrijksoverheid.nl/verwerkingen/-persoonsregistratie-en-nadere-inventarisatie-gevaarlijke-stoffen-(2021)

22. Grondslag. Bescherming van vitale belangen

Wat zegt de Autoriteit Persoonsgegevens over grondslag bescherming van vitale belangen:
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken#wanneer-mag-u-zich-baseren-op-de-grondslag-vitale-belangen-6343

23. Grondslag. Vervulling taak van algemeen belang of uitoefening van openbaar gezag

Wat zegt de Autoriteit Persoonsgegevens over grondslag algemeen belang of uitoefening van openbaar gezag.:
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken#wanneer-mag-u-zich-baseren-op-de-grondslag-algemeen-belang-of-openbaar-gezag-6329

24. Grondslag. Behartiging van de gerechtvaardigde belangen.

Wat zegt de Autoriteit Persoonsgegevens over grondslag behartiging van de gerechtvaardigde belangen:
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken#wanneer-mag-u-zich-baseren-op-de-grondslag-gerechtvaardigd-belang-6330

25. AVG. Adequaatheidsbesluit

Wat zegt de Autoriteit Persoonsgegevens over adequaatheidsbesluit?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal/doorgifte-binnen-en-buiten-de-eu#hoe-weet-ik-of-een-derde-land-een-passend-beschermingsniveau-heeft-1752

Gelijkaardige privacy aanpak voor EU, UK en AU?
Ja voor EU en VK:

- Voor gehele EU GDPR.
- De EC heeft 2 adequaatheidsbesluiten genomen voor het VK (1 voor de AVG en 1 voor de Richtlijn politie en justitie). Daarmee oordeelt de EC dat het niveau van bescherming van persoonsgegevens in het VK gelijkwaardig is aan dat in de EU.

Nee voor Australië, namelijk eigen wetgeving en bovendien geen EU adequaatheidsbesluit.

What privacy rules applies in Australia?
The Australian Privacy Principles (APPs) in schedule 1 of the Privacy Act, outline how most Australian Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses (collectively called 'APP entities') must handle, use and manage personal information.
The Privacy Act applies to businesses that are incorporated in Australia. It also applies to businesses outside Australia if they collect personal information from, or hold personal information in, Australia and carry on a business in Australia (s 5B of the Privacy Act).
The GDPR applies to 'personal data'. This means 'any information relating to an identified or identifiable natural person' (Article 4). This has similarities with the definition of 'personal information' in the Privacy Act, which is defined as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable' (s 6(1) of the Privacy Act).[12]
Under the GDPR, additional protections apply to the processing of 'special categories' of personal data, which includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (Article 9). Additional protections also apply to similar categories of 'sensitive information'[13] in the Privacy Act (for example, APP 3.3 (collection of solicited personal information), APP 6.2(a) (use or disclosure of personal information) and APP 7.4 (direct marketing)).
https://www.oaic.gov.au/privacy/guidance-and-advice/australian-entities-and-the-eu-general-data-protection-regulation

26. AVG. Algoritme

Wat zegt de Autoriteit Persoonsgegevens over algoritme?
Wat zegt de Autoriteit Persoonsgegevens verder over Algoritmes?

- https://www.autoriteitpersoonsgegevens.nl/themas/algoritmes-ai
- https://www.autoriteitpersoonsgegevens.nl/themas/algoritmes-ai/algoritmes-ai-en-de-avg
- https://www.autoriteitpersoonsgegevens.nl/themas/algoritmes-ai/algoritmes-ai-en-de-avg/regels-bij-gebruik-van-ai-algoritmes
- https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/ai-algoritmes
- https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/ai-algoritmes#faq
- https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/focus_ap_202-2023_groot.pdf

Overige

- https://algoritmeregister.amsterdam.nl/
- https://www.algoritmeregister.org/
- https://www.rotterdam.nl/bestuur-organisatie/algoritmeregister/
- https://www.stibbe.com/en/news/2021/july/towards-a-european-legal-framework-for-the-development-and-use-of-artificial-intelligence
- https://www.pwc.nl/nl/actueel-en-publicaties/themas/digitalisering/europese-ai-verordening-veel-procedurele-en-inhoudelijke-eisen.html
- https://www.ru.nl/rechten/studenten/actioma/actioma/alle-artikelen/bestuursrecht/betekent-voorstel-europese-ai-wet-nederlandse/
- https://vng.nl/nieuws/gemeenten-starten-met-een-algoritme-en-sensorenregister

Waar moet u aan voldoen als u met een algoritme persoonsgegevens verwerkt?
Een verwerking van persoonsgegevens met inzet van een algoritme is niet anders dan een ‘gewone’ verwerking. U moet daarom voldoen aan de algemene beginselen voor de verwerking van persoonsgegevens. Die beginselen staan in artikel 5 van de Algemene verordening gegevensbescherming (AVG). Belangrijke beginselen zijn onder meer:

1. Rechtmatigheid. U moet een grondslag hebben om persoonsgegevens te mogen verwerken (art. 6 AVG).
2. Transparantie.
    - Bij het verwerken van persoonsgegevens moet u transparant zijn richting de betrokkene (art. 12, 13 en 14 AVG). De betrokkene is degene van wie u gegevens verwerkt.
    - Ook heeft u een register van verwerkingsactiviteiten nodig (art. 30).
    - En gebruikt u een algoritmisch systeem voor bijvoorbeeld uw besluitvorming? Dan moet u nuttige informatie geven over de onderliggende logica en de verwachte gevolgen van die verwerking voor de betrokkene. Dit noemen we een algoritme register.
3. Doelbinding. U mag alleen persoonsgegevens verwerken voor een vooraf vastgesteld doel. U bent aan dit doel gebonden. Dit betekent dat u niet zomaar de persoonsgegevens voor een ander doel mag verwerken.
4. Dataminimalisatie. Verwerkt u persoonsgegevens voor een bepaald doel, dan moet u dit met zo min mogelijk persoonsgegevens doen. Alle gegevens die niet aantoonbaar nodig zijn,

verwerkt u onrechtmatig. U mag de gegevens ook maar beperkt opslaan. U moet hiertoe vooraf de bewaartermijnen vaststellen.
5. Juistheid. De persoonsgegevens die u verwerkt, moeten juist zijn (kloppen). Hiermee voorkomt u onvoorzienbare uitkomsten en ongewenste effecten voor de betrokkene.
6. Beveiliging. Alle persoonsgegevens die u verwerkt, moet u goed beveiligen. U moet hiervoor technische en organisatorische maatregelen treffen (art. 32 AVG). Daarbij moet u rekening houden met:
    - de stand van de techniek;
    - de aard, omvang, context en verwerkingsdoeleinden;
    - de uiteenlopende risico's voor de rechten en vrijheden van betrokkenen.
7. Privacy by design & default. Bij de ontwikkeling van (algoritmische) systemen moet u rekening houden met de principes privacy by design en privacy by default. Dit betekent dat u systemen privacyvriendelijk moeten ontwikkelen, inrichten en inzetten. Instellingen voor de gebruiker moeten standaard privacybeschermend zijn.

Wanneer treedt de AI Verordening in werking?
Hoewel de verordening waarschijnlijk pas in 2024 in werking treedt, is het raadzaam dat organisaties aan zich nu al voor te bereiden op de stroom aan beoordelingen, documentaties, certificeringen en dergelijke. ‘Uit onderzoek blijkt namelijk dat de volledige wetgeving honderden verplichtingen voor AI-operators bevat. Dat betekent dat organisaties met een hoop bureaucratisch werk te maken krijgen. Hoe eerder zij zich aanpassen aan de nieuwe AI-verordening, des te sneller ethische AI- en privacypraktijken in de systemen integreren.

Hoe voorbereiden op de AI Verordening?
Dit kan in vier stappen:
1. Breng het bestaan en gebruik van AI-systemen in organisatie en mogelijke ontwikkelingen die u in de komende jaren wilt doorvoeren in kaart.
2. Breid rollen uit om de verantwoordelijkheid van de AI-systemen te dragen. Naleving vereist het bewustzijn van juridisch, technisch en operationeel personeel. Onderschat het belang van cross-functionele rapportagelijnen en multidisciplinaire controles niet.
3. Implementeer een systeem van voortdurende risico-evaluatie binnen de activiteiten van uw organisatie.
4. Beheer de risico-evaluatie. Naarmate AI-systemen in de loop van de tijd evolueren, kan hetzelfde gebeuren voor de bijbehorende risico's. Eenmalige risicobeperking in het proces is daarom waarschijnlijk niet voldoende.

Zijn er boetes mogelijk bij non-compliance?
Ja, de boetes versterken het financiële aspect: een maximum van dertig miljoen euro of zes procent van de wereldwijde omzet, wat aanzienlijk hoger is dan de maximale AVG-boetes.’

27. AVG. Artificial Intelligence - AI

Wat zegt de AP over AI?
https://www.autoriteitpersoonsgegevens.nl/themas/algoritmes-ai

Wat zeggen andere bronnen?
https://www.ngfg.nl/nieuws/de-fg-en-ai-aflevering-1-arnoud-engelfriet
https://www.ngfg.nl/nieuws/de-fg-en-ai-aflevering-2-paulcollier

AI (Artificial Intelligence) en FG?
Een onderwerp waarmee iedere FG geconfronteerd wordt, is AI (Artificial Intelligence). Kunstmatige intelligentie (AI) belooft ons leven te veranderen en ons efficiënter, productiever, gezonder en innovatiever te maken. Deze technologie wordt al gebruikt in de private en publieke sector, waarbij de kracht van gegevens wordt ingezet om voorspellingen te verbeteren, betere producten en diensten te maken, kosten te verlagen en werknemers te bevrijden van routinematig administratief werk. Maar hoe zit het eigenlijk met de privacy en wat staat ons als FG's te wachten? Vanaf nu zullen wij maandelijks iemand aan de tand voelen over dit onderwerp. De eerste in deze reeks is Arnoud Engelfriet, Chief Knowledge Officer bij ICTRecht. We stelden hem 14 vragen.

1. Wie ben jij en wat doe jij precies?
Arnoud Engelfriet, ICT-jurist en partner bij adviesbureau ICTRecht. Ik leid daar de Academy en verzorg alle kennisdeling en opleidingen. Met mijn achtergrond in ICT ben ik dagelijks bezig met complexe vraagstukken over ict en recht, waar AI natuurlijk een belangrijk deel van uitmaakt. Ik schreef diverse boeken over technologie, privacy en recht, zoals ICT en Recht, de AVG: Artikelsgewijs Commentaar en het boek AI and Algorithms: Mastering Legal & Ethical Compliance dat in januari verschijnt.

2.Waarom was jij te porren voor dit interview over AI?
Door de eindsprint die de Europese AI Act nu trekt, is het onderwerp niet meer weg te denken. Iedereen moet nadenken over wat AI met hun organisatie doet, zowel de voordelen als de nadelen. En natuurlijk omdat ik al een half jaar bezig was met dat boek over ditzelfde onderwerp.

3. Welke wins zie jij in AI?
AI is automatisering van cognitieve taken, zeg maar van het traditionele denkwerk. De winst zit dan ook bij de inzet van AI om de saaie, vervelende cognitieve taken over te nemen. Ik ontwikkelde zelf in 2016 bijvoorbeeld een AI die geheimhoudingscontracten en verwerkersovereenkomsten screent op de belangrijkste pijnpunten. Dan weet je alvast dat alles erin staat dat belangrijk is, krijg je standaard commentaar voor de wederpartij op de dingen die anders moeten en tekstvoorstellen voor wat ontbreekt. Daarna moet je het zelf nog een keer lezen voor de rare dingen, maar de tijdsverdeling verschuift: niet 4 uur checken op standaardwerk en dan een half uurtje de rare dingen snelsnel doen, maar 2 minuten wachten op de check van DPA Lynn en daarna 2 uur een goede review of het wel past bij jouw situatie. Dat is een enorme win.
Ook bij andere zaken zoals het schrijven van teksten is AI heel waardevol. Het versnelt de standaard stappen zoals het vertalen van een leerdoel naar secties of bulletpoints voor je Powerpoint, het controleert en herschrijft je kladteksten in je eigen tone of voice en ga zo maar door. Een heel handig dingetje is bijvoorbeeld bronvermeldingen in de huisstijl van het tijdschrift te laten zetten. Bij cursussen helpt AI me om meerkeuzevragen (met antwoorden) te bedenken en casussen op te zetten.

4. Zoals bij iedere opkomende technologie zijn er ook risico's. Uit het wereldwijde onderzoek 2023 Trust in artificial intelligence blijkt dat 61 procent van de 17.000 ondervraagden op zijn/haar hoede is t.a.v. het vertrouwen in Ai-systemen. Slechts 50 procent gelooft dat de voordelen van Ai opwegen tegen de risico's. Over welke risico's hebben we het dan eigenlijk?
Vaak denken mensen bij risico's rond AI aan bias, vooringenomenheid met name in de vorm van discriminatie. Dat is zeker bij AI's die werken met persoonsgegevens een probleem, maar het is zeker niet het enige. Een zelfrijdende auto bijvoorbeeld zal niet snel discrimineren maar kan wel enorme schade en letsel geven. Een AI die examens nakijkt, kan fouten maken en daardoor verkeerde cijfers uitdelen. Een robot bij de apotheek kan verkeerde medicijnen verstrekken en letsel veroorzaken. Een verkeersregel-AI kan enorme files geven en ga zo maar door.
In mijn boek schets ik een evaluatie langs zeven assen die voor meer of minder risico kunnen zorgen. Deze komen uit de Ethische richtsnoeren voor betrouwbare KI van de Europese Commissie:

- menselijke controle en menselijk toezicht,
- technische robuustheid en veiligheid,
- privacy en datagovernance,
- transparantie,
- diversiteit, nondiscriminatie en rechtvaardigheid,
- milieu- en maatschappelijk welzijn en
- verantwoordingsplicht.

Afhankelijk van het systeem en de toepassing kies je per as hoe hoog je wilt scoren, en daar richt je je risicomanagement dan op in. Een medische AI moet bijvoorbeeld hoog scoren op controle en robuustheid, maar milieuwelzijn is secundair en nondiscriminatie zal minder snel spelen. Een AI die handelt in aandelen moet vooral heel robuust en transparant zijn maar heeft geen privacy-aspecten, en verantwoording afleggen is triviaal.

5. AI bevat enorme hoeveelheden (persoons)gegevens. Wat zijn naar jouw mening privacy-aspecten om rekening meet te houden bij AI?
Veel AI's, maar lang niet alle, worden gemaakt om met persoonsgegevens om te gaan. De AI die in aandelen handelt, zal bijvoorbeeld niets van personen hoeven te weten. En bij een AI die een auto bestuurt, spelen persoonsgegevens een heel andere rol dan bij een AI die fraude opspoort bij webwinkels of die tentamens op de universiteit nakijkt. Zie verder volgende vraag, maar de kern van het privacyprobleem ismeestal transparantie: hoe kon de AI dit over mij concluderen, waarom neemt de AI deze stap en hoe moeten we omgaan met de gevolgen voor mij als mens?

6. Hoe verhoudt AI zich tot de privacywetgeving? Wat betekent de AVG voor de ontwikkeling en toepassing van AI?
De AVG is niet perse een privacywet, maar gaat over een zorgvuldige omgang met je gegevens. Dat kan ook in de openbare ruimte zijn: een AI die jou op een groot scherm projecteert als hij ziet dat je door rood loopt, bijvoorbeeld. De AVG stelt strenge kaders aan AI's die omgaan met mensen. Allereerst moet je dataverzameling goed op orde zijn, wat een probleem is omdat AI's enorme datasets vereisen en er dus vaak snel en rommelig van alles bij elkaar geharkt wordt. Maar denk hierbij aan de grondslag en/of doelbinding, plus hoe je mensen informeert bij het samenstellen van de AI. Bias speelt een rol bij het inzetten van de AI, de problematiek hier is vergelijkbaar met artikel 22 AVG, de geautomatiseerde besluitvorming. Ook beveiliging, privacy by design en omgaan met opt-outs zijn aandachtspunten.

7. Privacy en Ai zijn dus onlosmakelijk met elkaar verbonden?
Nee. De AI Act heeft dat heel goed begrepen: die definieert een AI als een systeem dat autonoom handelt of ingrijpt en daarbij risico's opwerpt voor mens en maatschappij. Dat kan een privacyrisico zijn, maar ook een veiligheidsrisico (dood en letsel), financiële schade (verkeerde aandelen gekocht),

economische schade (contract verkeerd gelezen) of zelfs milieuschade. We moeten dus niet de fout maken AI als een AVG compliance issue te zien, of bij handelen van AI alleen het kader van artikel 22 (geautomatiseerde besluitvorming) te hanteren.

8. Hoe 'intelligent' is AI?
Ondanks de algemene perceptie dat AI-algoritmen op de een of andere manier neutraal en objectief zijn, kunnen ze bestaande, onbekende vooroordelen of onvolledigheden in gegevens vaak reproduceren en zelfs vergroten. Een in het oog springend voorval is natuurlijk de Toeslagaffaire. Maar wat zijn andere relevante voorbeelden?
De toeslagenaffaire is een slecht voorbeeld, omdat daar mensen bewust de keuze maakten om te discrimineren op afkomst. Een bekend voorbeeld van een biased AI is de recruitment tool van Amazon: die wees alle vrouwen af, omdat historisch het bedrijf alleen mannen in dienst had en er dus geen data was over succesvolle vrouwelijke medewerkers. Bij plaatjesgeneratoren zie je de bekende seksistische stereotypes: vraag om een dokter en je krijgt een man, vraag om een verpleegkundige en je krijgt een vrouw.
Belangrijk is te onthouden dat AI's niet denken zoals mensen dat doen, ze redeneren niet via logische regels of stappenplannen waarbij je kennis toepast. AI's trekken conclusies op basis van statistische analyse: dit plaatje lijkt op de tienduizend plaatjes die 'vogel' heten, dus dit is een vogel. Termen als 'intelligent' zijn dan ook gevaarlijk, want ze suggereren dat een AI menselijk denken kan vervangen. Wat je doet met inzet van AI is een proces automatiseren, maar net zoals een vorkheftruck niet hetzelfde werkt als een dokwerker, werkt een AI niet hetzelfde als een mens.

9. Waarom wordt er in discussies over AI zo vaak gehamerd op rekenschap ofwel accountability?
Rekenschap of verantwoording is een kernaspect van vertrouwen, en AI's moeten vertrouwen opbouwen om als technologie aanvaard te worden. Heel lang hebben AI's als zwarte dozen geopereerd: de computer zegt nee, en daar hebben we het mee te doen. AI systemen moeten nu dus vérgaand het omgekeerde doen: licht iedere stap toe, motiveer waarom dat een terechte stap is en verantwoord zo de inzet. Dit is meer dan transparantie: daar gaat het om wat het systeem doet, maar niet om waarom.

10. Een manier om privacy-risico's bij AI en Chatbots t voorkomen, is het toepassen van het principe Privacy by Design. Wat houdt dat precies in?
Privacy by design is het algemene beginsel dat je bij iedere ontwerpstap in een systeem rekening houdt met privacy en gegevensbescherming. Dit beginsel is natuurlijk ook van belang als je een AI systeem bouwt, zoals een chatbot. Het kan lastig zijn dit toe te passen omdat een AI systeem feitelijk een enorme bak van gegevens bevat waar statistische analyse op gedaan wordt, en dat is lastiger te begrenzen dan bijvoorbeeld een personeelsadministratiesysteem waarbij je inbouwt wie waar wel of niet bij mag.

11. Wanneer je gebruikt wilt gaan maken van algoritmische systemen waarbij persoonsgegevens worden verwerkt, ben je verplicht een DPIA (data protection impact assessment) uit te voeren. Wat is dat eigenlijk en wat zijn belangrijke criteria voor DPIA?
Een DPIA heeft als doel om de risico's van dergelijke verwerkingen in kaart te brengen en maatregelen te identificeren waarmee deze risico's te beperken zijn. Voor FG's zal dit dagelijkse kost zijn. Specifiek bij AI is het grootste probleem de risico's vorzien, want die kunnen heel anders uitpakken dan bij traditionele ict-systemen. Een voorbeeld is de zaak van mevrouw Pocornie, die zich anders behandeld zag door AI-gedreven antispieksoftware en vermoedde dat haar huidskleur daarin meespeelde: het systeem zei dat ze niet in beeld was terwijl ze wel voor de camera zat. Uiteindelijk bleek de slechte kwaliteit van haar webcam een factor van betekenis, maar dat is een risico waar maar weinig mensen vooraf op checken.

12. Wil je nog iets delen waarbij je het niet eens bent met veel andere FG's, de AP of anderen?
Wie AI systemen gaat beoordelen als FG moet zich voorhouden dat er meer aan zit dan alleen de AVG en omgang met persoonsgegevens. Ik denk dan ook dat een AI assessment breder moet zijn dan enkel een DPIA. Vertrouw verder niet op papieren of contractuele garanties dat bv. zorgvuldig en AVG-compliant persoonsgegevens zijn verwerkt, maar sta op een onafhankelijke controle en op daadwerkelijke inzage in de gebruikte data.

28. AVG. Blockchain

Wat zegt de AP over blockchain?
Geen inhoudelijke info over blockchain…

Bronnen:

- Whitepaper Juridische aspecten van Blockchain, Pels Rijcken & Droogleever Fortuijn, 16 november 2017 https://www.platformoutsourcing.nl › files › download › overig › whitepaper
- https://blogbestuursrecht.nl/experimenteren-met-blockchain-binnen-de-grenzen-van-de-wet/
- https://www.openrecht.nl/commentaar/b5810488-6e09-45d2-9f91-350214d79f15/

Worden er bij een blockchaintoepassing persoonsgegevens verwerkt?
Als persoonsgegevens worden gelogd in een blockchain is daarop de AVG van toepassing en moet dus aan de daarin gestelde regels worden voldaan. Om die reden wordt er soms voor gekozen om niet de persoonsgegevens zelf, maar een zogenaamde hash van persoonsgegevens in een blockchain te plaatsen. Een hashfunctie is simpel gezegd een wiskundige formule die tekst omzet in een cijferreeks en die als uniek kenmerk heeft dat vanaf de cijferreeks niet teruggerekend kan worden naar de tekst. Als we het hebben over een hash van persoonsgegevens hebben we het dus over de cijferreeks die ontstaat door de persoonsgegevens om te zetten met behulp van de wiskundige formule. Uit een advies van de Artikel 29-werkgroep (samenwerkingsorgaan van de Europese privacytoezichthouders; thans de European Data Protection Board) lijkt te volgen dat het hashen van persoonsgegevens niet leidt tot een situatie waarin gegevens niet meer herleidbaar zijn tot natuurlijke personen. Om die reden lijkt er vooralsnog van te moeten worden uitgegaan dat met hashen van persoonsgegevens de AVG niet buiten werking kan worden gesteld, al bestaat op het advies van de Artikel 29-werkgroep wel de nodige kritiek.

Wanneer sprake van het verwerken van persoonsgegevens binnen een blockchain?
De Algemene Verordening Gegevensbescherming (AVG) is vaak van toepassing indien sprake is van het verwerken van persoonsgegevens. Op grond van artikel 4 lid 1 van de AVG zijn persoonsgegevens alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Dat betekent dat onder meer naam, adresgegevens en telefoonnummers persoonsgegevens zijn, maar dat dit ook kan gelden voor een set andere gegevens die gezamenlijk iets zeggen over een geïdentificeerde of identificeerbare natuurlijke persoon, zoals locatiegegevens of videobeelden. Als dergelijke informatie is opgenomen in een blockchain, is sprake van persoonsgegevens.
Van het verwerken van persoonsgegevens is op grond van artikel 4 lid 2 van de AVG onder meer sprake bij het verzamelen, vastleggen, ordenen, structureren en opslaan van persoonsgegevens. Indien persoonsgegevens worden gelogd in een blockchain zal in de regel altijd sprake zijn van het verwerken van persoonsgegevens.
Gegevens die volledig geanonimiseerd zijn en waarvoor dus geldt dat zij niet meer te herleiden zijn tot een geïdentificeerde of identificeerbare natuurlijke persoon, zijn geen persoonsgegevens. Als een blockchain uitsluitend anonieme gegevens bevat, is geen sprake van persoonsgegevens en is het privacyrecht niet van toepassing.

Hoe kwalificeren de verschillende betrokken partijen? Als verwerkingsverantwoordelijke, verwerker, betrokkene en/of derde?
Alle deelnemers aan een blockchain waarbinnen persoonsgegevens worden uitgewisseld, kwalificeren in de regel als verwerkingsverantwoordelijke in de zin van de AVG. Wij kunnen ons

voorstellen dat de partijen die alleen nodes draaien binnen een blockchainnetwerk kwalificeren als verwerkers. De primaire taak van deze partijen is immers het laten functioneren van de blockchain ten behoeve van alle verwerkingsverantwoordelijke deelnemers. Als de partijen die nodes draaien daadwerkelijk verwerkers zijn, dan zijn de verwerkingsverantwoordelijken verplicht om met deze verwerkers verwerkersovereenkomsten te sluiten (artikel 28 AVG). Hiervoor geldt dat dit binnen een blockchain waarin een zekere vorm van governance bestaat, is op te lossen door daarover tussen alle deelnemers en de partijen die de nodes draaien gezamenlijke afspraken te maken.

Wie is verantwoordelijke en verwerker binnen een blockchain?
Indien persoonsgegevens binnen een blockchain verwerkt worden, zullen deze persoonsgegevens door de verschillende deelnemers binnen een blockchain in de blockchain geplaatst worden. In feite is dit niet meer dan een innovatieve manier van het uitwisselen van persoonsgegevens tussen de verschillende deelnemers binnen een blockchain. Bij deze uitwisseling is in beginsel geen sprake van een hiërarchische relatie; als daarover geen andere afspraken zijn gemaakt is iedere deelnemer aan de blockchain gelijk en staat het in beginsel iedere deelnemer vrij om met de informatie in de blockchain te doen wat hem of haar goed dunkt. Van een verwerker is bij het delen van persoonsgegevens via een blockchain volgens ons dan in beginsel ook geen sprake. Dat betekent dat alle partijen die deelnemen aan blockchain verantwoordelijke zijn.

Hoe kan aan de materiële eisen van de AVG worden voldaan?
De uitgangspunten en voordelen van blockchaintechnologie bijten in meer of mindere mate met de beginselen van gegevensbescherming uit de AVG. Zo is de kern van blockchaintechnologie dat sprake is van onveranderbare, niet verwijderbare data die staat opgeslagen op meerdere plekken. De materiële eisen van de AVG zijn daartegen gebaseerd op de beginselen van dataminimalisatie, juistheid van gegevens en opslagbeperking (zie artikel 5 AVG). Staat de AVG daarmee aan de weg aan de inzet van blockchain?
Niet zonder meer, zeker niet wanneer gebruik wordt gemaakt van een (meer) gesloten blockchain. Een blockchain kan meer gesloten zijn, bijvoorbeeld doordat vastligt welke partijen de nodes beheren waaruit de blockchain bestaat, welke partijen toegang krijgen tot een blockchain of welke informatie partijen kunnen zien binnen een blockchain. Vaak wordt een gesloten blockchain beheerd door een organisatie. Dat doet af aan de oorspronkelijke bedoeling van blockchain om trusted third parties overbodig te maken, maar heeft voordelen in termen van gegevensbescherming.
Zo kan bij een (meer) gesloten blockchain, waarbij deelnemende partijen en partijen achter nodes bekend zijn, onder meer afspraken worden gemaakt over de omgang met de rechten van betrokkenen, zoals met verzoeken om gegevens te wissen en te rectificeren.
Bovendien biedt blockchain juist ook mooie kansen voor het uitoefenen van de rechten van betrokkenen en het geven van vrije, specifieke, geïnformeerde toestemming, doordat die rechten kunnen worden ingeregeld in de techniek.

Grondslag voor het verwerken van persoonsgegevens binnen een blockchain?
Voor iedere verwerking van persoonsgegevens dient een aparte grondslag te bestaan. Dat betekent dat ieder keer dat een deelnemer aan een blockchain daarin persoonsgegevens plaatst, voor deze verstrekking een grondslag dient te bestaan.

Dataminimalisatie en blockchain?
De AVG vereist dat sprake dient te zijn van dataminimalisatie, hetgeen betekent dat niet meer persoonsgegevens worden verwerkt dan strikt noodzakelijk voor het doel van de blockchain. Een oplossing die recht doet aan dit beginsel is dat in de logs voornamelijk metagegevens (dat-informatie)

worden opgenomen en de inhoudelijke gegevens (wat-informatie) slechts via een link worden toegevoegd die enkel door geautoriseerde personen kan worden geopend.

Het verwijderen van persoonsgegevens uit een blockchain?
De kracht van de blockchain is dat op de juistheid van de informatie daarin vertrouwd kan worden omdat deze informatie onveranderbaar is. Dat botst met het gegeven dat de AVG bepaalt dat zodra persoonsgegevens niet meer nodig zijn, deze verwijderd moeten worden en dat betrokkenen op grond van de AVG het recht hebben om te verzoeken om verwijdering van hun persoonsgegevens. Voor het verwijderen van informatie uit een blockchain is een meerderheid van het aantal nodes vereist. Indien in een gesloten blockchain één partij de macht over alle of in ieder geval de meerderheid van de nodes heeft, is het voor deze partij dus mogelijk om informatie uit de blockchain te verwijderen. Sceptici zullen zich daarbij direct afvragen wat dan nog de waarde is van de blockchain. Hoewel zij uiteraard een punt hebben, kan als er goede afspraken gemaakt worden over de governance van de gesloten blockchain toch een constructie gerealiseerd worden waarbij op de juistheid van de blockchain vertrouwd kan worden.
Aan verwijderen kunnen uiteraard ook technische eisen gesteld worden. Zo is bijvoorbeeld denkbaar dat een blockchain zo geprogrammeerd wordt dat verwijdering alleen mogelijk is door de betreffende persoonsgegevens te versleutelen en de sleutel vervolgens weg te gooien. In een dergelijk geval blijven de versleutelde gegevens wel zichtbaar. Bovendien zou een extra log kunnen worden toegevoegd met de mededeling dat gegevens zijn versleuteld. In een dergelijk geval is weliswaar sprake van de verwijdering van gegevens, maar blijft toch zichtbaar dat er ooit iets gelogd is in de blockchain.

Het aanpassen van persoonsgegevens binnen een blockchain?
Op grond van de AVG hebben betrokkenen niet alleen het recht om te verzoeken om verwijdering van persoonsgegevens, maar ook om aanpassing van onjuiste persoonsgegevens. Hierbij loopt men tegen vergelijkbare bezwaren aan als bij de verwijdering van persoonsgegevens. Toch is het vermoedelijk relatief eenvoudig om deze bezwaren weg te nemen. Zo kunnen wij ons voorstellen dat persoonsgegevens die zich in de blockchain bevinden niet zozeer worden aangepast door een oude log te wijzigen, maar door een nieuwe log aan de blockchain toe te voegen waarin de eerdere gegevens worden gecorrigeerd. In een dergelijk geval wordt het onveranderlijke karakter van de blockchain niet aangetast.

Stroomschema voor blockchain?

Stroomschema toepasselijkheid Europese privacyregels voor blockchain

29. AVG. Brexit

Wat zegt de AP over Brexit?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal/brexit

Bron: https://www.ploum.nl/kenniscentrum/nieuws/brexit-en-de-verwerking-van-persoonsgegevens-onder-de-avg-wat-verandert-er

Geeft u als organisatie in de Europese Unie (EU) persoonsgegevens door aan organisaties in het Verenigd Koninkrijk (VK)?
Dan kunt u dat blijven doen zoals u gewend bent. Ook al maakt het VK geen deel meer uit van de EU. De Brexit heeft dus geen gevolgen voor de doorgifte van gegevens van de EU naar het VK. Dat heeft de Europese Commissie (EC) op 28 juni 2021 besloten.
Vanaf 1 januari 2021 tot 28 juni 2021 gold een overgangsperiode. In deze periode kon u ook gegevens doorgeven aan het VK zoals u gewend was. En dat blijft nu dus zo.

Adequaatheidsbesluiten VK?
De EC heeft 2 adequaatheidsbesluiten genomen voor het VK (1 voor de AVG en 1 voor de Richtlijn politie en justitie). Daarmee oordeelt de EC dat het niveau van bescherming van persoonsgegevens in het VK gelijkwaardig is aan dat in de EU.
Dat betekent dat u vrij gegevens kunt uitwisselen met het VK. U hoeft dus geen doorgifte-instrumenten te gebruiken zoals een modelcontract, wat u normaal nodig zou hebben voor doorgifte naar een land buiten de EU.

Gegevens ontvangen uit VK?
Organisaties in de VK kunnen vrij persoonsgegevens versturen naar organisaties in de EU. Dat heeft de Britse regering laten weten. Dus ontvangt u gegevens uit het VK? Dan heeft de Brexit ook daarop geen invloed.

Zie verder de website van de Britse privacytoezichthouder:
https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/international-data-transfers/

30. AVG. Centrum Informatiebeveiliging en Privacybescherming (CIP)

Wat zegt AP over CIP?
Geen informatie.

Wat is het CIP?
Centrum Informatiebeveiliging en Privacybescherming is een publiek-private netwerkorganisatie die bestaat uit Participanten en Kennispartners. Participanten zijn overheidsbedrijven waarvan medewerkers meedoen aan een of meer van de werkverbanden binnen de samenwerking. Kennispartners zijn marktpartijen die met een convenant verbonden zijn en een hoeveelheid uren hebben toegezegd in de samenwerking. Werken op basis van 'voor allen, door allen'.

Wat doet het CIP?
CIP organiseert en faciliteert kennisdeling in vele vormen, zoals themabijeenkomsten, workshops en games en biedt een reeks van producten aan die iedereen kan downloaden en (tenzij anders vermeld) vrij gebruiken onder de Creative Commons licentie Naamsvermelding-Gelijk Delen. Producten vrij te downloaden en gebruiken.
https://www.cip-overheid.nl/productcategorie%c3%abn-en-worshops/producten/gegevens-bescherming/

Welke producten?
O.a. bewustwording
https://www.cip-overheid.nl/media/1661/20210817-pdc-cip-def.pdf

31. AVG. Certificatie

Wat zegt AP over certificatie?

- https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/avg-certificaat
- https://www.autoriteitpersoonsgegevens.nl/actueel/avg-certificering-komt-stap-dichterbij

Wat zegt commerciële partij over certificatie?

- https://brandcompliance.com/en/product/gdpr-certification-standard/
- https://www.privacycompany.eu/blogpost-nl/het-ene-certificaat-is-het-andere-niet

Welke privacy certificaten zijn er?
Er zijn erg veel privacy gerelateerde standaarden en certificaten bekend in de markt. De meest bekende zijn onder meer: ISO 27701, EuroPrise, BS 10012, BC 5701, CARPA, EuroPrivacy. Het meest bekende certificaat is waarschijnlijk de ISO 27701 een privacy add-on van de ISO 27001-reeks.

Privacy certificaat of AVG certificaat?
Niet elk privacy certificaat kan het ook effectief schoppen tot AVG certificaat. In de artikelen 42 en 43 van de AVG staan de regels waaraan een standaard moet voldoen om als AVG certificaat erkend te kunnen worden. Bovendien moet een standaard niet enkel voldoen aan de voorwaarden die in de AVG zijn opgenomen, het moet ook formeel worden goedgekeurd door de European Data Protection Board (EDPB). Een erkend AVG certificaat zal ook worden opgenomen in een register van de EDPB.

Zijn er dan nog geen AVG certificaten voorhanden?
Het register van de EDPB is momenteel nog leeg. Dit betekent dat er nog geen AVG certificatiestandaarden zijn goedgekeurd. Maar in 2023, vijf jaar na het in werking treden van de AVG zal daar verandering in komen.

Voldoet ISO27001 of BS10012?
Neen, ISO 27701 en ook BS 10012 voldoen niet aan de voorwaarden zoals opgenomen in artikel 42 en 43 van de AVG. Beide standaarden zijn opgebouwd volgens ISO 17021 en niet zoals de geëiste ISO 17065 standaard. EuroPrise een standaard uit Duitsland biedt privacy certificering voor IT-producten en -diensten, maar is tot op heden enkel lokaal goedgekeurd. Echter zijn er 3 standaarden goed op weg om effectief erkend te worden als het eerste AVG certificaat.

CARPA (Luxemburg)
Deze standard is de eerste goedgekeurd standaard in Luxemburg. CARPA is ontwikkeld en wordt beheerd door de Luxemburgse toezichthouder. De CNPD is tot dusver de enige Europese toezichthoudende autoriteit die zelf een certificeringsregeling in het kader van de AVG heeft ontwikkeld. Als de entiteit die de certificeringscriteria heeft ontwikkeld, is de CNPD ook de eigenaar van de certificeringsregeling. Hierdoor is het CARPA schema een certificaat met vooral waarde in Luxemburg.

EuroPrivacy (Luxemburg)
De autoriteit in Luxemburg is zeer actief de laatste maanden en zet alles op alles om het eerste AVG certificaat naar Luxemburg te halen. Zo werd naast de CARPA standaard de AVG standaard van EuroPrivacy eind 2022 goedgekeurd door de Luxemburgse toezichthouder en de EDPB. Alleen is er voor deze standaard (nog) geen goedgekeurd certificatieschema ontwikkeld. EuroPrivacy heeft een gesloten netwerk van partners en als je als organisatie gecertificeerd wil worden (wanneer het certificatieschema eenmaal is goedgekeurd) dient een welkomst pack te worden aangekocht.

BC 5701 (Brand Compliance – Nederland)?
Maar ook in Nederland staat er een AVG certificaat in de startblokken. Sinds 2017 investeert Brand Compliance in een AVG certificaat. Deze standaard werd volledig ontwikkeld volgens de vereisten uit de artikelen 42 en 43 van de AVG. Brand Compliance heeft de uitgebreide audit ervaring ingezet om een standaard te ontwikkelen die geschikt is voor elk type organisatie. In de zomer van 2022 heeft Brand Compliance een positief ontwerpbesluit ontvangen namens de Autoriteit Persoonsgegevens. In september 2022 werd de goedkeuringsaanvraag ingediend bij de EDPB. De goedkeuring van de EDPB wordt nog voor de zomer verwacht. Naast de standaard heeft Brand Compliance ook steeds een certificatieschema en een bijhorende handleiding ontwikkeld. Brand Compliance heeft ervoor gekozen de standaard en het schema zo op te bouwen zodat het haalbaar en betaalbaar is voor elk type van organisatie. Door de intensieve ontwikkeling, de volledigheid en diverse signalen is het niet vreemd als binnen enkele maanden in Nederland het eerste geldige AVG certificaat wordt uitgereikt.

Status AVG certificatie BC 5701 volgens de AP?
De AVG biedt de mogelijkheid om verwerkingen te certificeren. Hiermee kunt u naleving van de AVG aantonen. De AP heeft recent de certificeringsstandaard van Brand Compliance goedgekeurd (Certification Standard and Criteria BC 5701:2023). Dit is een belangrijke stap in het goedkeuringsproces, maar het is nog niet mogelijk om bij Brand Compliance een AVG-certificaat aan te vragen. Brand Compliance moet hiervoor eerst nog worden geaccrediteerd door de Raad van Accreditatie. Heeft u vragen over het verloop van die procedure? Neem dan contact op met Brand Compliance. Mogelijk kunt u al starten met de voorbereidingen voor een certificeringsproces. Brand Compliance kan u hierover informeren. Op termijn zullen meer aanbieders AVG-certificeringen aanbieden.

32. AVG. Cybersecurity

Wat zegt AP over Cybersecurity?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/beveiliging-van-persoonsgegevens

Bron: https://www.dirkzwager.nl/media/21816/cyberverzekeringen-vanuit-rechtsvergelijkend-perspectief-privacyregelgeving-in-de-vs-en-de-europese-avg.pdf

Verzekering Cybersecurity wegens de AVG?
Cyberverzekeringen zijn in de Verenigde Staten al tientallen jaren op de markt.2 In de VS is de privacyregelgeving met haar meldplichten en boetes voor een belangrijk deel de motor achter de vraag naar verzekeringsdekking voor cyberrisico's. De voornaamste reden om deze verzekering af te sluiten is gelegen in (compliance) kosten rondom een 'datalek'. Het Amerikaanse privacyrecht verschilt evenwel sterk van de Europese regelgeving.

Creëert de inhoud van de AVG dezelfde behoefte aan specifieke cyberverzekeringsdekking als de Amerikaanse privacyregelgeving?
Deels.
Het Amerikaanse privacy recht verschilt sterk van de Europese regelgeving. De vraag naar de cyberverzekering in de VS wordt grotendeels gedreven door zeer specifieke privacyregelgeving, waarin een grote nadruk ligt op het voldoen aan die regelgeving (compliance), meldplichten na datalekken en grote schades door boetes en aansprakelijkheid. Dit creëert een verzekeringsbehoefte waar de cyberverzekering op aansluit, bijvoorbeeld door dekking te verlenen voor aansprakelijkheid, kosten van verweer en kosten rondom datalekken, zoals notificatiekosten.
In de AVG is in grote lijnen een beweging naar het Amerikaanse model te zien. De AVG roept daarmee deels dezelfde behoefte aan specifieke verzekeringsdekking op. De in Nederland aangeboden cyberverzekeringen sluiten daar in beginsel goed op aan. Indien sprake is van een datalek, schrijft de AVG een risicoanalyse voor die de onderneming in zeer korte tijd dient uit te voeren. Niet ieder datalek hoeft immers te worden gemeld. Cyberverzekeringen bieden hierin ondersteuning door middel van incident response services. Met het oog op compliance kunnen deze diensten voor verzekeringnemers zeer waardevol zijn.

In hoeverre sluit de thans in Nederland aangeboden cyberverzekering op de AVG aan?
In Europa wordt de cyberpolis slechts door een select groepje verzekeraars aangeboden. De getoetste onderdelen zijn ingekaderd naar de hiervoor benoemde drijfveren: compliance en kosten rondom (de
meldplicht) datalekken, boetes en aansprakelijkheid.

- Compliance en kosten rondom meldplicht datalekken. Compliance en verantwoording zijn belangrijke thema's in de AVG. Vertaald naar verzekeringsdekking is dit element met name te zien rondom de meldplicht datalekken. Een
  voorbeeld daarvan is het feit dat alle getoetste polissen voorzien in incident response services. Daarmee kan de aangeboden dekking voor de verwerkingsverantwoordelijke een middel vormen om in geval van een datalek aan de AVG te voldoen. Verzekerden kunnen aanspraak maken op crisismanagement, juridische ondersteuning bij de beoordeling of de inbreuk meldingsplichtig is, of juist voor de communicatie met de overheid. De technische ondersteuning kan bestaan uit forensische of IT-diensten die de oorzaak van de inbreuk vaststellen136 of herstelwerkzaamheden uitvoeren. Verder bieden alle getoetste polissen dekking voor het opzetten van een callcenter om betrokkenen van informatie te voorzien, al

is daar in een enkele polis voorafgaande toestemming van de verzekeraar voor nodig. Dekking voor deze diensten is met het oog op de 72-uurstermijn uit de AVG in Europa zeer wenselijk. De verzekerde kan gebruikmaken van het netwerk van specialisten van de verzekeraar, wat een grote tijdbesparing kan opleveren. Het wordt daarmee voor hem een stuk beheersbaarder om te voldoen aan de eisen van de AVG rondom het melden van datalekken.

- Boetes. Waar in Amerikaanse cyberpolissen de boete een veelvoorkomende uitsluiting is, valt de handhavingsboete die de toezichthouder (in Nederland de Autoriteit Persoonsgegevens) kan opleggen veelal wel onder de dekking van de in Nederland aangeboden cyberverzekeringen. Sporen van die Amerikaanse uitsluitingen zijn ook terug te zien in de in Nederland aangeboden polissen. Zo is in meerdere polissen opgenomen dat van dekking is uitgesloten 'regulerende boetes' of 'regelgevingsboetes', terwijl de eventuele boete van de AP wel is gedekt. Ondanks dat het vooralsnog de vraag blijft hoe vaak deze boetes werkelijk zullen worden opgelegd en dus hoe reëel de dreiging daarvan is en of boetes in het licht van artikel 3:40 BW wel verzekerbaar zijn, sluit deze dekking thans goed aan op een behoefte die de AVG creëert.
- Aansprakelijkheid. In een enkele polis wordt onderscheid gemaakt tussen schade bij een privacy gerelateerde onrechtmatige daad, die wordt beperkt tot personenschade, en schade voortvloeiend uit een privacy claim. In de meeste polissen wordt evenwel een algemeen schadebegrip gebruikt ('schade voortvloeiend uit een gedekte aanspraak'). Alle polissen bieden dekking voor de kosten van verweer, zowel tegen aansprakelijkheidsclaims als tegen een boetebesluit door de Autoriteit Persoonsgegevens

Moet de klager ook bewijslast aanleveren?
Elk persoon kan een klacht indienen bij de Autoriteit Persoonsgegevens. Deze zullen in behandeling genomen moeten worden. Dit kan een klacht zijn omdat er niet gereageerd wordt, of dat er twijfels zijn over de data die opgegeven is. Of dat er het vermoeden is dat de gegevens langer bewaard worden dan is aangegeven. De bewijslast ligt dan bij het aangeklaagde bedrijf om te bewijzen dat de processen en documentatie in orde is. Dat is de reden dat de AVG documenten essentieel zijn. Omdat hieruit moet blijken hoe je je processen op orde hebt.

Waar is de AP aan gebonden bij de uitvoering?
De Autoriteit Persoonsgegevens is bij de uitvoering van zijn taken gehouden aan de bepalingen van de Algemene wet bestuursrecht. Dat betekent onder meer dat:

- tegen besluiten van de Autoriteit Persoonsgegevens bezwaar kan worden gemaakt en beroep kan worden aangetekend bij de bestuursrechter;
- de Wet openbaarheid van bestuur van toepassing is;
- een klacht over de Autoriteit Persoonsgegevens kan worden ingediend bij de Nationale ombudsman;
- de Autoriteit Persoonsgegevens als bestuursorgaan uiteraard ook gebonden is aan de algemene beginselen van behoorlijk bestuur.

Hoe opereert de AP in Europees verband?
De AP maakt deel uit van de Artikel 29-werkgroep, waarin de Europese privacy toezichthouders zijn verzameld. De Autoriteit Persoonsgegevens draagt binnen deze werkgroep bij aan de totstandkoming van gezamenlijke opinies en standpunten. Ook houdt de Autoriteit Persoonsgegevens zich in dit verband bezig met de nieuwe Europese privacyregelgeving.

Hoe/wanneer weten organisaties zeker dat ze aan de AVG voldoen?
Er bestaat niet zoiets als een audit voor de AVG. Het is uiteindelijk de verantwoordelijkheid van organisaties zelf om de wet na te leven. De Autoriteit Persoonsgegevens werkt wel veel samen met brancheorganisaties en doet veel aan voorlichting.

Hoe is de bestuurlijke handhaving van de Algemene verordening gegevensbescherming (AVG) vormgegeven?
Op 25 mei 2018 treedt de Algemene verordening gegevensbescherming ("AVG") in werking. De verordening heeft rechtstreekse werking in het Nederlandse rechtssysteem. Het gevolg daarvan is dat de Nederlandse privacywaakhond, de Autoriteit Persoonsgegevens, een scala handhavingsinstrumenten op grond van de AVG kan inzetten om naleving van de privacywetgeving te bevorderen. Thans behandelt de Eerste Kamer de Uitvoeringswet Algemene verordening gegevensbescherming ("UAVG"). Beoogd wordt om de UAVG op 25 mei 2018 in werking te laten treden. De UAVG geeft nadere uitvoering aan de AVG die op sommige aspecten aan lidstaten ruimte laat om bepaalde aspecten nader te regelen. De UAVG bevat in aanvulling op en ter uitvoering van de AVG onder meer een aantal belangrijke voorschriften die zien op handhaving. Als gevolg van de inwerkingtreding van de AVG en de UAVG is de Wet bescherming persoonsgegevens ("Wbp") niet meer van toepassing. In deze FAQ zullen wij een aantal vragen die in de praktijk spelen over bestuurlijke handhaving onder de AVG en UAVG nader bespreken.

Welke instantie is in Nederland bevoegd tot handhaving van de AVG?
De AVG bepaalt dat iedere lidstaat van de Europese Unie één of meer toezichthouders moet oprichten, die belast zijn met het toezicht op de Verordening (artikel 51, eerste lid, AVG). In Nederland is dit de Autoriteit Persoonsgegevens (artikel 6, tweede lid, UAVG).

Welke handhavingsinstrumenten heeft de Autoriteit Persoonsgegevens op grond van de AVG en UAVG?
De AVG vergroot en verzwaart het arsenaal aan handhavingsinstrumenten dat de Autoriteit Persoonsgegevens thans op grond van de Wbp heeft. De AVG biedt de toezichthouder de mogelijkheid om zogeheten 'corrigerende maatregelen' (artikel 58, tweede lid, AVG) op te leggen. Daarnaast biedt de UAVG de Autoriteit Persoonsgegevens ook de mogelijkheid tot oplegging van een last onder bestuursdwang of een last onder dwangsom (artikel 16 UAVG).
Onder 'corrigerende maatregelen' in de AVG vallen onder meer:

- waarschuwing
- berisping
- administratieve geldboete, oftewel een bestuurlijke boete
- tijdelijke of definitieve verwerkingsbeperking (waaronder een verwerkingsverbod)
- intrekking van certificaten
- opschorting van gegevensstromen naar een ontvanger in een derde land.

De UAVG 'vertaalt' de term 'corrigerende maatregelen' met uitzondering van de waarschuwing als 'bestuurlijke sancties' in de zin van de Algemene wet bestuursrecht (artikel 14, vierde lid, UAVG). Dat betekent dus dat de bepalingen uit de Awb die zien op de bestuurlijke sancties ook van toepassing zijn op de desbetreffende corrigerende sancties in de AVG. Daarbij kan bijvoorbeeld gedacht worden aan de cumulatie van corrigerende sancties (artikel 5:6 Awb) en dat deze sancties preventief kunnen worden opgelegd (artikel 5:7 Awb).

Is de Autoriteit Persoonsgegevens verplicht om handhavend op te treden?
De (U)AVG verplicht de Autoriteit Persoonsgegevens niet om handhavend op te treden. Bovendien verplicht deze wetgeving de Autoriteit niet om voor een bepaald handhavingsinstrument (bijvoorbeeld een boete of last onder dwangsom) te kiezen. Het gaat om discretionaire

bevoegdheden die de toezichthouder ruimte laten om zelf handhavingsbeleid te bepalen en in dat kader prioriteiten te kiezen.
Het zou vanwege de rechtszekerheid van betrokken partijen goed zijn wanneer de Autoriteit Persoonsgegevens in beleidsregels duidelijk maakt onder welke omstandigheden zij handhavend zal optreden en in welke gevallen zij van een bepaald instrument gebruik zal maken.

Hoe hoog zijn de boetes die de Autoriteit Persoonsgegevens maximaal kan opleggen?
De AVG biedt de Autoriteit Persoonsgegevens de bevoegdheid om hoge boetes op te leggen wegens specifieke inbreuken op de AVG. Artikel 83 AVG voorziet in de sanctionering met boetes in twee categorieën overtredingen:
….
Of de Autoriteit Persoonsgegevens daadwerkelijk maximale boetes zal gaan opleggen, is de vraag. Het gaat daarbij om maatwerk. De hoogte van de boete zal in elk geval afhangen van verschillende omstandigheden, zoals de aanwezigheid van opzet, het zijn van first offender, het behaalde financieel voordeel etc. (artikel 83, tweede lid, AVG). Ook het evenredigheidsvereiste speelt daarbij een belangrijke rol (artikel 3:4 lid 2 en artikel 3:46 Awb).

Wie kan worden geconfronteerd met handhaving?
De Autoriteit Persoonsgegevens kan handhavend optreden tegen degene tot wie de normen zich in de AVG richten. Dat zijn de ‘verwerkingsverantwoordelijke’ (artikel 4, zevende lid, AVG), de ‘verwerker’ (artikel 4, achtste lid, AVG), en de ‘vertegenwoordiger van de niet in de Unie gevestigde verwerkingsverantwoordelijke of verwerker’ (artikel 4, zeventiende lid, AVG). Dat betekent dat elke onderneming, overheidsinstelling of natuurlijk persoon normadressaat van de AVG kan zijn en dus met handhaving kan worden geconfronteerd.

Welke bestuursrechtelijke rechtsbescherming staat open tegen sancties van de Autoriteit Persoonsgegevens?
Een belanghebbende kan zich tegen een door de Autoriteit Persoonsgegevens opgelegde bestuurlijke sanctie verweren. Alvorens een sanctie wordt opgelegd, wordt eerst een ontwerpbesluit opgesteld waartegen een zienswijze mogelijk is. Wordt een sanctie opgelegd, dan kan daartegen een bezwaarschrift bij de Autoriteit Persoonsgegevens worden ingediend. Tegen het besluit op bezwaar van de Autoriteit Persoonsgegevens staat beroep bij de rechtbank open in eerste aanleg en hoger beroep bij de Afdeling bestuursrechtspraak van de Raad van State. Is sprake van een spoedeisende situatie dan kan een voorlopige voorziening hangende bezwaar, beroep en hoger beroep bij de bestuursrechter worden ingediend. De bestuursrechter kan daarbij prejudiciële vragen stellen aan het HvJ EU. Na afronding van de nationale procedure kan de vraag naar de rechtmatigheid van de sanctie onder het EVRM aan het EHRM worden voorgelegd.

Schort de indiening van bezwaar of beroep de werking van een bestuurlijke sanctie op?
Nee, tenzij het gaat om een bestuurlijke boete. Net als onder de Wbp gaat de UAVG er vanuit dat het indienen van een bezwaarschrift bij de Autoriteit Persoonsgegevens en een beroepschrift bij de rechtbank tegen de opgelegde bestuurlijke boete schorsende werking heeft. De bestaande regeling in de Wbp is daarmee in de UAVG gehandhaafd. Dat betekent dat de boete in afwachting van de procedure bij de Autoriteit Persoonsgegevens en in beroep bij de rechtbank niet behoeft te worden betaald (artikel 38 UAVG). Voor andere bestuurlijke sancties, zoals de berisping of het verwerkingsverbod, geldt geen schorsende werking; daarvoor zou eventueel een voorlopige voorziening uitkomst kunnen bieden.

Zal de Autoriteit Persoonsgegevens na 25 mei 2018 meteen boetes uitdelen?
Minister Dekker van Rechtsbescherming heeft op 8 maart 2018 in een debat met de Tweede Kamer gezegd dat de Autoriteit Persoonsgegevens niet direct boetes zal gaan uitdelen als op 25 mei 2018 de nieuwe privacyregels in werking treden. Dat zal voor bedrijven, overheden en instellingen mogelijk een opluchting zijn. Volgens Dekker zal de Autoriteit Persoonsgegevens zich de eerste maanden vooral richten op voorlichting. Echter, de Autoriteit Persoonsgegevens is onafhankelijk toezichthouder dus afgewacht moet worden hoe deze opmerking in de praktijk zal uitwerken.

33. AVG. Verantwoordingsplicht/ Documenten

Wat zegt de Autoriteit Persoonsgegevens over verantwoordingsplicht?
Zie: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/verantwoordingsplicht
En
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/controle-over-je-data

Welke documenten heb je verplicht nodig om de AVG te voldoen?

1. Register van verwerkingsactiviteiten;
2. Data protection impact assessment (DPIA) voor gegevensverwerkingen met een hoog privacyrisico;
3. Register van datalekken die zijn opgetreden;
4. Het aantonen dat een betrokkene daadwerkelijk toestemming heeft gegeven voor een gegevensverwerking wanneer u voor een verwerking toestemming nodig heeft.
5. Functionaris voor gegevensbescherming onderbouwen waarom u ervoor gekozen hebt om al dan niet een FG aan te stellen.
6. Data privacy beleid. Onder de AVG hebben organisaties een informatieplicht, zij moeten nieuwe of bestaande klant, etc. duidelijk informeren over wat zij met uw persoonsgegevens doen, bijvoorbeeld via een heldere online privacyverklaring.

Welke extra maatregelen laten zien dat je aan de AVG voldoet?
Naast de verplichte maatregelen kan een bedrijf ervoor kiezen om extra maatregelen te nemen waarmee je aantoont dat je voldoet aan de eisen van de AVG. De AP noemt bijvoorbeeld:

1. het aansluiten bij een gedragscode; MAAS is niet aangesloten bij een gedragscode
2. het behalen van een bepaald certificaat; MAAS heef geen specifiek AVG certificaat
3. het hanteren van een specifiek ICT-beveiligingsbeleid; …
4. het afleggen van verantwoording over de verwerking van persoonsgegevens in uw jaarverslag of in een speciaal privacy-jaarverslag; MAAS legt jaarlijks in ieder geval verantwoording af in het MVO jaarverslag. Een jaarverslag door de FG wordt onderzocht.

Hoewel deze maatregelen niet verplicht zijn, helpen zij u wel om aan de toezichthouder te laten zien dat een bedrijf voldoet aan de eisen van de AVG. Daarom moedigt de AP deze vrijwillige maatregelen aan.

Hoe zorg ik er voor dat mijn organisatie aan de AVG blijft voldoen?
De Autoriteit Persoonsgegevens (AP) gaf eerder dit jaar een zestal aanbevelingen om te voldoen aan de verantwoordingsplicht (het principe van ‘accountability’). Sinds de AVG dient iedere organisatie namelijk te voldoen aan die verantwoordingsplicht. Onder de verantwoordingsplicht valt bijvoorbeeld het aanleggen (en bijhouden) van een verwerkings- en datalekkenregister, het uitvoeren van data protection impact assessments, het bewaren van toestemming gegeven door de betrokkene en het aanstellen van een Functionaris Gegevensbescherming (FG). Om aan de verantwoordingsplicht te (blijven) voldoen kan uw organisatie een gegevensbeschermingsbeleid opstellen.

Maar wat moet er nu precies in zo’n gegevensbeschermingsbeleid staan? En is dat weer wat anders dan de privacyverklaring? Hierna vindt u meer informatie over het gegevensbeschermingsbeleid, het verschil met een privacyverklaring en tips om uw gegevensbeschermingsbeleid op orde te houden.

Wat is een gegevensbeschermingsbeleid?
Het gegevensbeschermingsbeleid is een beleidsdocument waarin de verwerkingsverantwoordelijke technische en organisatorische maatregelen heeft neergelegd om de rechten van betrokkenen te waarborgen. Een gegevensbeschermingsbeleid is hetzelfde als een privacy beleid, maar niet hetzelfde als een privacyverklaring of privacy statement. Met dit beleidsdocument kunt u laten zien aan de AP dat uw organisatie voldoet aan de verantwoordingsplicht, mits goed opgesteld en uitgevoerd.
Organisaties die verplicht zijn om een FG aan te stellen, dienen een gegevensbeschermingsbeleid op te stellen. Verder is het afhankelijk van de aard en de omvang van de verwerkingen van uw organisatie of u verplicht bent om een gegevensbeschermingsbeleid op te stellen. Het kan echter voor elke organisatie nuttig zijn. Met dit beleidsdocument brengt u namelijk alle verwerkingen binnen uw organisatie in kaart en heeft u goed overzicht waar waarborgen of extra maatregelen getroffen kunnen worden.

Wat moet er in mijn gegevensbeschermingsbeleid staan?
Een voordeel van het gegevensbeschermingsbeleid is dat alle privacy gerelateerde zaken in één document zijn vastgelegd. Zorg er voor dat de volgende onderdelen niet ontbreken:

- Een omschrijving van de categorieën persoonsgegevens die worden verwerkt;
- De doeleinden waarvoor u de persoonsgegevens verwerkt;
- De getroffen maatregelen (waaronder technische en organisatorische maatregelen) om de gegevens te beschermen;
- (Een link naar) uw verwerkingsregister (uw databoekhouding);
- Hoe uw organisatie voldoet aan de beginselen van verwerking van persoonsgegevens zoals die in de AVG staan vermeld;
- Bewaartermijnen van de verschillende categorieën persoonsgegevens;
- Protocol meldplicht datalekken incl. een register waarin de datalekken worden bijgehouden;
- De rechten die betrokkenen kunnen uitvoeren en hoe zij dat kunnen doen.

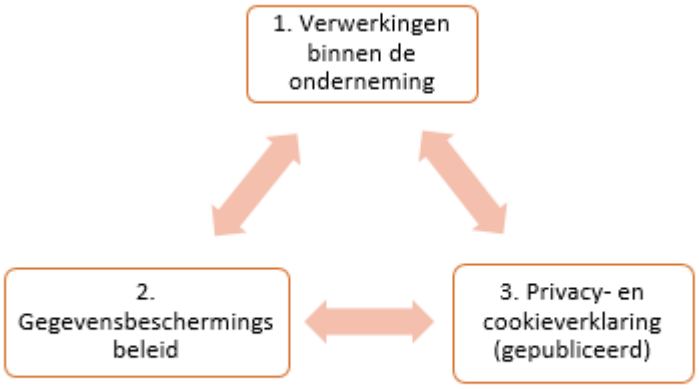
Wellicht heeft uw organisatie al het een en ander van deze informatie hebben vastgelegd, bijvoorbeeld in een informatiebeveiligingsbeleid, een data retentiebeleid, een protocol meldplicht datalekken, enz. Het gegevensbeschermingsbeleid kan in dat geval een overzicht geven hoe deze documenten met elkaar samenhangen, als een soort handleiding.

Verschil gegevensbeschermingsbeleid en privacyverklaring?
Het verschil tussen het gegevensbeschermingsbeleid en de privacyverklaring is het doel waarvoor beide documenten gebruikt worden. Met het gegevensbeschermingsbeleid voldoet uw organisatie aan haar verantwoordingsplicht. Met de privacyverklaring voldoet uw organisatie aan de transparantieplicht (ook wel informatieplicht). Meer informatie over de informatieplicht vindt u in een eerder bericht hier.

Tips voor een optimaal gegevensbeschermingsbeleid?

- Wees concreet: maak de vertaalslag van papier naar de praktijk. Zorg dat de juiste collega’s/adviseurs weten wat zij moeten doen in geval van bijvoorbeeld een datalek.
- Publiceer uw gegevensbeschermingsbeleid (deels) online. Zo is het voor betrokkenen duidelijk voor welk doel en hoe hun persoonsgegevens verwerkt worden. Let op dat u geen procedures omtrent de beveiliging deelt.
- Controleer periodiek bij de business of managementlagen of de organisatie onlangs is gestart of gestopt met bepaalde verwerkingen. Pas het gegevensbeschermingsbeleid van uw organisatie daar op aan. Onderstaand schema geeft u inzicht of uw gegevensbeschermingsbeleid op orde is, dan komt de informatie in alle drie de kaders

namelijk met elkaar overeen. Zorg ervoor dat deze wisselwerking gesloten blijft en er geen losse eindjes ontstaan.



Bron:

- https://www.ploum.nl/verantwoordingsplicht-hoe-zorg-ik-er-voor-dat-mijn-organisatie-aan-de-avg-blijft-voldoen/

34. AVG. Plichten Verwerkingsverantwoordelijke

Wat zegt de AP over plichten verwerkingsverantwoordelijke?
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/voorbeeldlijst_verwerkers_def.pdf

Wie is wanneer verantwoordelijk en waarvoor?
De AVG spreekt van verantwoordelijken en verwerkers. Wanneer u data (persoonsgegevens) aan MAAS verstrekt bent u de 'verantwoordelijke'. MAAS is hierbij de 'verwerker'. De verstrekking en de verwerking van de data moet in een overeenkomst zijn vastgelegd (de verwerkersovereenkomst). In de rol van verantwoordelijke dient MAAS aan te tonen dat u de juiste technische en organisatorische maatregelen heeft genomen om de persoonsgegevens te beschermen.

Wat zijn de verwerkingsbeginselen voor de verwerkingsverantwoordelijke?
Op grond van de Verordening moet elke verwerking van persoonsgegevens voldoen aan de volgende beginselen:

- de verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn ("rechtmatigheid, behoorlijkheid en transparantie");
- de verwerking moet gebonden zijn aan specifieke verzameldoelen ("doelbinding");
- de persoonsgegevens moeten toereikend zijn, ter zake dienend, en beperkt tot wat noodzakelijk is ("minimale gegevensverwerking");
- de gegevens moeten juist zijn ("juistheid");
- de gegevens mogen niet langer worden bewaard dan nodig ("opslagbeperking");
- gegevens moeten goed beveiligd zijn en vertrouwelijk blijven ("integriteit en vertrouwelijkheid").

De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van deze beginselen.

Wat zijn de plichten van de verwerkingsverantwoordelijke?
De verwerkingsverantwoordelijke moet ook kunnen aantonen dat een verwerking van persoonsgegevens aan deze beginselen voldoet (de verantwoordingsplicht). Concreet dient de verwerkingsverantwoordelijke hiertoe:

- een register van verwerkingsactiviteiten bij te houden (de registerplicht);
- onder bepaalde omstandigheden een functionaris voor gegevensbescherming aan te stellen;
- voorafgaand aan risicovolle verwerkingsactiviteiten een gegevensbeschermingseffect-beoordeling uit te voeren;
- de Autoriteit Persoonsgegevens onder bepaalde omstandigheden voorafgaand aan een nieuwe risicovolle verwerkingsactiviteit te raadplegen (voorafgaande raadpleging);
- bij het inrichten van verwerkingen rekening te houden met het principe van privacy door ontwerp en standaardinstellingen (privacy by design & default);
- passende beveiligingsmaatregelen te treffen met het oog op de bescherming van persoonsgegevens;
- in het geval van een datalek melding te doen bij de Autoriteit Persoonsgegevens en onder bepaalde omstandigheden ook bij de betrokkenen;
- afspraken te maken met verwerkers:
- medewerking te verlenen aan de Autoriteit Persoonsgegevens;
- de rechten van de betrokkenen te respecteren en in te vullen.

35. AVG. Plichten Verwerker

Wat zegt de AP over plichten verwerker?
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/voorbeeldlijst_verwerkers_def.pdf

Wat is een verwerker?
Van een "verwerker" is sprake als de derde de persoonsgegevens ten behoeve van de werkgever als verantwoordelijke verwerkt. Een eigen MAAS werknemer wordt daarbij overigens niet als een verwerker beschouwd. Niet iedere derde die in opdracht van de werkgever persoonsgegevens verwerkt is een verwerker. Als een derde zelf verantwoordelijk is voor de verwerking van de persoonsgegevens (dat wil zeggen: als hij zelf het doel en de middelen van de verwerking van de persoonsgegevens vaststelt), dan is die derde geen verwerker. Deze derde zal geen verwerkersovereenkomst met u willen sluiten, omdat hij dan niet meer in staat is de op hem of haar rustende verantwoordelijkheid voor de verwerking van de persoonsgegevens te nemen.

Waar moet je als verwerker op letten, welke eisen worden er door de AVG gesteld?
Een aantal in het oog springende vereisten waarmee de verwerker rekening dient te houden. Deze vereisten worden onder meer in art. 28 AVG genoemd.
Verwerkers mogen uitsluitend handelen in opdracht van de verantwoordelijke en de persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke. Dit geldt ook met betrekking tot de doorgiften van persoonsgegevens aan een derde land of aan een internationale organisatie, tenzij er een op de verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling is die hem tot verwerking verplicht. Wanneer deze situatie zich voordoet stelt de verwerker de verwerkingsverantwoordelijke, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.
De verwerker dient te waarborgen dat de "tot het verwerken van de persoonsgegevens gemachtigde personen" zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden.
Verwerkers dienen op grond van art. 32 AVG passende technische- en organisatorische beveiligingsmaatregelen te nemen die een passend beschermingsniveau bieden, rekening houdend met risico van de gegevensverwerking voor betrokkenen. Verwerkers dienen hiervoor een goede kennis te hebben inzake hun informatiesystemen en de typen van data die zij verwerken.
Je mag als verwerker niet zondermeer nieuwe sub-bewerkers inschakelen zonder dat er hiervoor toestemming is verkregen van de verantwoordelijke. In het geval van een algemene schriftelijke toestemming licht de verwerker de verwerkingsverantwoordelijke vooraf in over veranderingen inzake de toevoeging of vervanging van sub-verwerkers. Hierbij dient de verwerkingsverantwoordelijke de mogelijkheid te worden geboden om tegen de veranderingen bezwaar te maken.
De verwerker krijgt tevens een zorgplicht waarbij hij de verwerkingsverantwoordelijke bijstand dient te verlenen bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36. Het gaat hier om zaken zoals beveiliging, meldplicht datalekken, en uitvoeren PIA. Zo moeten je als verwerker de verantwoordelijke "onverwijld op de hoogte stellen van een datalek". De termijn voor onverwijld moet nog worden bepaald.
Daarnaast ben je als verwerker verplicht om medewerking te verlenen bij een verzoek daartoe van de Autoriteit Persoonsgegevens (AP) in het kader van de uitoefening van diens taken. In bepaalde gevallen moet je als verwerker, voorafgaand aan de verwerking van persoonsgegevens, de AP

consulteren of een Privacy Impact Assessment uitvoeren. In bepaalde situaties is het als verwerker noodzakelijk om zelf een Data Protection Officer (DPO) aan te stellen. Dit is bijvoorbeeld het geval wanneer de bewerker een publieke organisatie is, wanneer er bij de verwerking sprake is van op grote schaal reguliere en systematische monitoring van betrokkenen of wanneer de primaire activiteit van de verwerking bestaat uit het op grote schaal verwerken van bijzondere persoonsgegevens.
Als verwerker dien je op voorhand een “exit-procedure” overeen te komen. Hierin spreek je op voorhand af hoe je na afloop van de verwerkingsdiensten, naargelang de keuze van de verwerkingsverantwoordelijke, de persoonsgegevens wist of terugbezorgt, en bestaande kopieën verwijdert.

Heb je als verwerker een documentatieplicht?
Als verwerker heb je een documentatieplicht. Als verwerker dien je hierdoor een register bij te houden van alle categorieën van verwerkingsactiviteiten die ten behoeve van een verwerkingsverantwoordelijke zijn verricht. Als verplichte onderdelen binnen het register noemt art. 30 AVG onder meer:

- de naam en de contactgegevens van de (sub-)verwerkers en van iedere verwerkingsverantwoordelijke voor rekening waarvan de verwerker handelt en indien van toepassing van de DPO;
- de categorieën van verwerkingen die voor iedere verwerkingsverantwoordelijke zijn uitgevoerd;
- doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, onder vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, bedoelde doorgiften, de documenten inzake de passende waarborgen;
- een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen zoals genoemd in art. 32 lid 1.

Is er een boetebeding voor verwerkers?
De AVG kent een boetebeding in het geval van een inbreuk op (onder meer) art. 28 AVG. Deze administratieve boetes kunnen oplopen tot 10 miljoen euro of tot 2% van de wereldwijde jaaromzet van een onderneming. Indien een verwerker in strijd met de AVG handelt, wordt die verwerker onverminderd de artikelen 82, 83 en 84 met betrekking tot die verwerking als de verwerkingsverantwoordelijke beschouwd. De boetes kunnen hierdoor uiteindelijk oplopen tot 20 miljoen euro of 4% van de wereldwijde jaaromzet van een onderneming.

Wat zijn de plichten van de verwerker?
De belangrijkste plichten op grond van de Verordening voor de verwerker zijn:

- de verwerker mag alleen handelen in opdracht van de verwerkingsverantwoordelijke;
- de verwerker wordt verplicht een overzicht bij te houden van alle categorieën persoonsgegevens die hij verwerkt in opdracht van de verwerkingsverantwoordelijke (registerplicht);
- de verwerker moet passende technische en organisatorische beveiligingsmaatregelen nemen die een passend beschermingsniveau bieden met het oog op het risico van de gegevensverwerking voor betrokkenen;
- de verwerker mag geen sub-verwerkers inschakelen zonder toestemming van de verwerkingsverantwoordelijke;
- de verwerker moet de verwerkingsverantwoordelijke onverwijld op de hoogte stellen van een datalek;

- de verwerker is verplicht medewerking te verlenen bij een verzoek van de toezichthouder (Autoriteit Persoonsgegevens) in het kader van de uitoefening van diens taken;
- de verwerker dient in bepaalde gevallen een functionaris voor gegevensbescherming aan te stellen.

36. AVG. Intern beheer

Wat zegt de Autoriteit Persoonsgegevens over intern beheer?
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/avg_brochure_wat_betekent_het_voor_jou_als_ondernemer.pdf

Overige informatie?
https://mxi.nl/kennis/320/intern-beheer-bij-inhuur-de-escape-in-de-avg

Wat is intern beheer?
“Wanneer u ondergeschikt bent aan de verwerkingsverantwoordelijke of er anderszins sprake is van een hiërarchische verhouding (u bent bijvoorbeeld medewerker, gedetacheerd bij de verwerkingsverantwoordelijke of een ZZP’er die werkt onder de instructies van uw opdrachtgever), dan is er geen sprake van verwerkerschap. In Nederland wordt deze situatie aangeduid als intern beheer “.
Deze term, "intern beheer" (handleiding AVG 3.5.1), zorgt op dit moment vooral voor veel discussies bij opdrachtgevers en publieke AVG/GDPR fora op LinkedIn. Vooral de term willen gebruiken om maar geen afspraken met elkaar vast te leggen of juist te verzanden in onhaalbare of onbegrijpelijke afspraken. Bij aanpassingen van de WBP eind jaren 1990 was de definitie van de "bewerker" niet voldoende uitgewerkt. De term "intern beheer" is daarom gedefinieerd en opgenomen in een memorie van toelichting (in kamerstukken 25 892 P61).
Intern beheer gaat over personen die voor de informatieveiligheid en privacy verantwoordelijke (verwerkingsverantwoordelijke) werken. Zij hebben een beperkte hiërarchische afstand tot de verantwoordelijke en zijn soms niet een directe werknemer. Eenvoudiger, deze persoon is niet in staat doel en middelen voor de verwerking zelf te bepalen. De verwerkingsverantwoordelijke oefent direct gezag uit.

37. AVG. Privacy by Design

Wat zegt de Autoriteit Persoonsgegevens over Privacy by Design:
Zie: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacycheck/privacy-design

Wie hebben er binnen MAAS toegang tot persoonsgegevens en wat gebeurt hiermee?
Zie daarvoor de bijlage *Informatiebeveiligingsbeleid MAAS* bij de verwerkersovereenkomst.

Waar moet je op letten bij een uitwisseling van persoonsgegevens met verantwoordelijke?
Een uitwisseling met een partij die kwalificeert als verantwoordelijke is een "verwerking" die moet voldoen aan alle eisen die de wet stelt. Voorbeeld: het doorzenden van gegevens van personeelsleden aan een pensioenfonds, het doorzenden van gegevens aan de leasemaatschappij, het doorzenden van een dossier aan een opvolgend behandelaar. Er zal dus een grondslag voor de verwerking moeten zijn, de verwerking zal in overeenstemming moeten zijn met het doelbindingsbeginsel, de verwerking zal goed beveiligd moeten zijn en de transparantie zal moeten zijn gewaarborgd. De betrokkene mag verantwoordelijke ook rechtstreeks aanspreken op de wijze waarop deze omgaan met diens persoonsgegevens.

Wat zegt de AVG over logbestanden?
Daarin wordt met geen woord over logbestanden gesproken. Wel legt de AVG de verplichting op om alle datalekken rondom persoonsgegevens te documenteren. Die documentatieplicht gaat ver want deze omvat ook alle feiten omtrent een dergelijk incident, de gevolgen daarvan en de genomen corrigerende maatregelen. Het belang van die documentatie is ook groot. De toezichthouder (AP) kan die desgewenst opvragen. Een bedrijf of organisatie kan aan die documentatieplicht feitelijk niet voldoen als er geen adequate logbestanden zijn. De wetgeving rondom datalekken voorziet dus in een loggingsverplichting, ook al wordt die term in dat verband niet uitdrukkelijk gebruikt. Het ligt dus voor de hand dat de toezichthouder ook logbestanden kan opvragen.

Wat zijn de maatregelen rond logbestanden?
Logbestanden bevatten niet zelden persoonsgegevens, zoals de IP-adressen van de gebruikers van het betrokken IT-systeem. In dat geval gelden voor de logbestanden zelf ook weer de spelregels rondom integriteit en beveiliging, bewaartermijnen en het wissen en vernietigen van deze bestanden. Met die impliciete verplichting te loggen is de mate van breedte en diepgang van logging nog niet duidelijk. De AVG zwijgt daarover. Aan de hand van denkbare risico's van het systeem en de betrokken belangen van burgers zal ieder bedrijf en organisatie daarover van geval tot geval zelf een specifieke afweging moeten maken. Dat is dus maatwerk. Indien softwareontwikkeling aan een derde partij wordt uitbesteed, zal dus goede aandacht moeten worden gegeven aan het maken van de specificaties daarover.

Bron:
https://security-architect.com/how-to-assess-security-maturity-and-roadmap-improvements/
(geraadpleegd 18-09-2019)

38. AVG. Data in de cloud

Wat zegt de AP over data de cloud?
https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-stelt-geen-onderzoek-naar-opslag-medische-gegevens-cloud

Bron: https://www.computable.nl/artikel/blogs/cloud-computing/6363162/5260614/zeven-fabels-over-cloudstorage-en-de-avg.html

Is data in de cloud versleuteld en dus kan niemand er ongeoorloofd bij?
De term encryptie wordt vaak gebruikt om persoonsgegevens te beschermen en/of een datalek te voorkomen. Encryptie kan inderdaad een oplossing bieden, maar moet daarbij wel op de juiste manier zijn toegepast. De data kan namelijk op twee manieren worden verstuurd: 'in transit', wat over een beveiligde verbinding betekent, of 'at rest', wat inhoudt over het systeem waar de data opgeslagen wordt. Ook kan het zijn dat er een applicatie gebruikt wordt die de data versleutelt nog voordat het naar de cloud gaat. Het is belangrijk om te vragen wie deze encryptiesleutels beheert. En aan wie deze rechten eigenlijk worden verleend. Is er een sleutel nodig bij het opstarten van een (storage-)systeem, zoals bij het gebruik van self encrypted disks? Kortom, met alleen het gebruik van encryptie bent je er nog niet. Het kan een goed beveiligingsmiddel zijn mits het doel en de implementatie juist zijn, maar de beveiliging is niet direct gegarandeerd. Zorg er voor dat deze informatie helder is.

Mogen alleen in Nederland data worden opgeslagen?
Niet alleen Nederland heeft te maken met de AVG/ GDPR: elke organisatie binnen de Europese Unie moet voldoen aan de privacywetgeving; politie, justitie en inlichtingendiensten hebben eigen wetgeving. Zelfs organisaties van buiten Europa die diensten in Europa aanbieden zijn verplicht om aan de AVG/ GDPR te voldoen. Door de harmonisering in heel de EU van het regelement in bescherming van persoonsgegevens én het vrije verkeer van gegevens maakt het dus niet uit waar de persoonsgegevens worden opgeslagen. Overal gelden dezelfde sancties bij het overtreden van de regels. Er is geen wet die voorschrijft dat de data niet in een ander land dan Nederland mag worden opgeslagen. Ook de NEN7510, BIR en BIG schrijven het niet voor.

Kan ik mijn data opslaan waar ik wil in de cloud?
U bent in alle gevallen verplicht om de cloud storage provider te controleren op de naleving van de AVG. Waar u uw data, met specifiek daarin (bijzondere) persoonsgegevens, ook opslaat, u bent te allen tijde verantwoordelijk voor de bescherming hiervan. Andere regels zoals de BIR, BIG en NEN7510 waar uw organisatie wellicht ook mee te maken heeft gelden ook nog naast de AVG. Belangrijk is dus om te controleren of uw storageprovider voldoet aan dezelfde normering als uw organisatie, omdat deze de verwerker is van de persoonsgegevens waar u de verantwoording over heeft. Dit kunt u controleren door bij uw provider op te vragen of zij ISAE3402 gecertificeerd zijn.

Zijn onze data in de cloud altijd beschermd tegen virussen en ransomware?
Onthoud dat als er toegang is tot de data, een virus ook toegang kan krijgen tot deze data. In het geval van een virus maakt het niet uit of data in het eigen datacenter of in de cloud is opgeslagen. Als een systeem (pc of server) geïnfecteerd is en een mountpoint, LUN, share of bucket in de cloud heeft, kan de data in de cloud net zo gemakkelijk worden versleuteld of corrupt worden gemaakt. De data in de cloud is dus niet automatisch beschermd tegen virussen en ransomware.

Is er geen back-up meer nodig als onze data in de cloud staan?
Tenzij de data zelf een back-up is of kopie hiervan, moet er in (bijna) alle gevallen nog steeds een back-up worden gemaakt van de data in de cloud. Vaak wordt gebruikgemaakt van oudere versies van bestanden en een prullenmand voor verwijderde items van de laatste dertig dagen. Dit alleen biedt onvoldoende bescherming om een langere periode te overbruggen. Ook is het hierbij bijna niet mogelijk om een beleid op alle gebruikers toe te passen. Meer redenen om zelf uw back-up te beheren zijn bijvoorbeeld het zelf in staat zijn te wisselen van provider en te migreren van back-updata, het gebruiken van ow back-upkopie voor disaster/recovery-doeleinden en voor search/datamining en data-analyses.
Het is belangrijk om aan te kunnen tonen welke persoonsgegevens waar bewaard worden en dat de gegevens verwijderd zijn als een persoon hierom heeft gevraagd of zodra de persoonsgegevens niet meer relevant zijn. Zonder data- of back-up-managementapplicatie is dat onhaalbaar.

Heb ik geen verwerkersovereenkomst voor de AVG nodig als wij data in de cloud bewaar?
Er is een verwerkersovereenkomst nodig wanneer er data met persoonsgegevens voor verwerking uitbesteed wordt aan een verwerker. Een verwerker is iemand die persoonsgegevens verwerkt ten behoeve van de verantwoordelijke, zonder rechtstreeks aan zijn of haar gezag te zijn onderworpen. Onder verwerking vallen veel handelingen met betrekking tot persoonsgegevens, bijvoorbeeld verzamelen, ordenen, bijwerken, verspreiden, samenbrengen, wijzigen, raadplegen, vastleggen, bewaren. Het bewaren en opslaan van data met persoonsgegevens vereist een bewerkersovereenkomst tussen de verwerker en de verantwoordelijke. Voor data in de cloud geldt dit dus ook.

Hoef je een datalek niet te melden bij de Autoriteit Persoonsgegevens als de data in de cloud is versleuteld?
Dit is onjuist. Het is belangrijk dat een datalek binnen 72 uur gemeld wordt bij de Autoriteit Persoonsgegevens zodra er persoonsgegevens zijn verloren of als er ongeautoriseerd toegang is verkregen tot deze gegevens. De gedupeerden moeten namelijk worden ingelicht en gewaarschuwd worden over het ongunstige feit dat hun gegevens openbaar zijn geworden. Een lek kan vervelende gevolgen hebben voor de personen waar de gegevens van gelekt zijn, ook wel de betrokkenen genoemd. De Autoriteit Persoonsgegevens kan aanwijzingen geven over het omgaan met een lek.

Als je de juiste technische en organisatorische maatregelen neemt, ziet de AP dan geen beletsel om (medische) data bij Google, Amazon of Microsoft op te slaan?
Maar dat gaat veel te ver, zegt een woordvoerder van de AP desgevraagd. Zou je dan op zijn minst mogen zeggen dat er in dit specifieke geval vanuit de AVG geen principieel bezwaar bestaat tegen de opslag van (Nederlandse medische) data op de servers van Google? Zelfs die conclusie kun je niet trekken, zegt de AP. De feitelijke mededeling dat er “geen aanleiding is tot het instellen van verder onderzoek” zegt precies wat er wordt bedoeld, en verdere duiding over hoe de AP tegen Amerikaanse cloud-providers aan kijkt kun je er niet uit halen, aldus de woordvoerder. Gezond verstand vertelt je dat, als MRDM de AVG zou overtreden door met Google in zee te gaan, de AP wel een vervolgonderzoek zou instellen. Maar zo stellig zul je het de AP dus niet horen zeggen.
Die gegevens zijn volgens MRDM opgeslagen in het datacentrum van Google in Eemshaven. Ze blijven volgens de minister “daarmee in Nederland en vallen onder Nederlandse en Europese wet- en regelgeving.” Volgens de contracten die MRDM met Google heeft gesloten, mag Google niet aan de data komen, zei Bruins. Google is gecertificeerd onder het zogeheten EU-US Privacy Shield. Dit is, zegt de minister, een adequaat mechanisme voor naleving van de vereisten van de Europese wetten inzake gegevensbescherming, vooral wanneer die te maken hebben met de overdracht van persoonlijke gegevens van de Europese Unie naar de Verenigde Staten. MRDM zei daarnaast de data dubbel te versleutelen, dus een versleuteling door Google en een eigen versleuteling, waarmee de

gegevens niet toegankelijk zijn voor Google. Tenslotte, stelde de brief naar de kamerleden, is geregeld dat wanneer beheerders van Google zich vanuit beheerswerkzaamheden toegang verschaffen tot de versleutelde gegevens, MRDM daar melding van krijgt, zodat gecontroleerd kan worden dat Google zich aan wettelijke en contractuele bepalingen houdt.

39. AVG. Data Protection Impact Assessment (DPIA)

Wat zegt de Autoriteit Persoonsgegevens over DPIA?
Zie https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia

Andere bronnen:
https://compliance-instituut.nl/media/jlth1bod/dco_41_lr_web.pdf

Wat is een DPIA?
Een data protection impact assessment (DPIA) is een instrument om privacy risico's van een gegevensverwerking in kaart te brengen, zodat een organisatie passende maatregelen kan nemen om de risico's te verkleinen.

Waarom zijn DPIA's belangrijk?
DPIA's zijn belangrijk voor een organisatie:

a. Om het benodigde inzicht in verwerkingen te verkrijgen.
   Om de privacybelangen van betrokkenen (b.v. haar klanten, cliënten, patiënten, burgers, leerlingen, medewerkers etc.) te kunnen beschermen, moet zij inzicht hebben in de (privacy)risico's van haar dataverwerkende processen.
b. Om aan te kunnen tonen dat voor privacyrisico's in processen passende beheersmaatregelen zijn genomen.
c. Omdat deze op grond van de AVG verplicht zijn bij processen met hoge privacyrisico's voor betrokkenen.

Op welk tijdstip moeten ze worden uitgevoerd?
Art. 35 lid 1 AVG is duidelijk: 'vóór de verwerking'. Dit is ook in lijn met de door de AVG voorgeschreven aanpak van Privacy by Design en Privacy by Default. Het idee van toch maar alvast starten met een verwerking en daarna een DPIA uitvoeren gaat in tegen de AVG en maakt een organisatie kwetsbaar voor acties vanuit de Autoriteit Persoonsgegevens (AP) en claims van betrokkenen. Een organisatie is namelijk verplicht bij hoog risico privacy verwerkingen voor de start van de verwerking de risico's voor betrokkenen voldoende te mitigeren met beheersmaatregelen.

Wanneer is uitvoeren van DPIA verplicht?
Niet uitputtende lijst is aangegeven in het *Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is, Autoriteit Persoonsgegevens*
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf van 27 november 2019.
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-uitkering/controle-van-personeel#welke-voorwaarden-gelden-voor-de-heimelijke-controle-van-werknemers-4621

Welke daarvan relevant voor MAAS?
1. Heimelijk onderzoek
Grootschalige verwerkingen van persoonsgegevens en-of stelselmatige monitoring waarbij informatie wordt verzameld door middel van onderzoek zonder de betrokkene daarvan vooraf op de hoogte te stellen (bijvoorbeeld: heimelijk onderzoek door particuliere recherchebureaus, onderzoek in het kader van fraudebestrijding en onderzoek op internet in het kader van bijvoorbeeld online handhaving van auteursrechten). Een gegevensbeschermingseffectbeoordeling (DPIA) is ook

verplicht in geval van heimelijk cameratoezicht door werkgevers in het kader van diefstal- of fraudebestrijding door werknemers (bij deze laatste verwerking dient ook in incidentele gevallen een gegevensbeschermingseffectbeoordeling (DPIA) te worden uitgevoerd vanwege de ongelijkwaardige machtsverhouding tussen de betrokkene (werknemer) en de verwerkingsverantwoordelijke (werkgever)). [3], [5], [7]
2. Zwarte lijsten
Verwerkingen waarbij persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten, gegevens over onrechtmatig of hinderlijk gedrag of gegevens over slecht betalingsgedrag door bedrijven of particulieren worden verwerkt en gedeeld met derden (artikel 33, vierde lid, aanhef en onder c, van de Uitvoeringswet Algemene verordening gegevensbescherming)(zwarte lijsten of waarschuwingslijsten, zoals deze bijvoorbeeld gebruikt worden door verzekeraars, horecabedrijven, winkelbedrijven, telecomproviders alsook zwarte lijsten die betrekking hebben op onrechtmatig gedrag van werknemers, bijvoorbeeld in de zorg of door uitzendbureaus). [4], [6], [7], [8]
7. Gezondheidsgegevens
Grootschalige verwerkingen van gegevens over gezondheid (bijvoorbeeld door instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, arbodiensten, reïntegratiebedrijven, (speciaal)onderwijsinstellingen, verzekeraars, en onderzoeksinstituten) waaronder ook grootschalige elektronische uitwisseling van gegevens over gezondheid (let wel: individuele artsen en individuele zorgprofessionals zijn op grond van overweging 91 van de Algemene verordening gegevensbescherming uitgezonderd van de verplichting een gegevensbeschermingseffectbeoordeling (DPIA) uit te voeren). [4], [5], [7]
11. Controle werknemers
Grootschalige verwerking van persoonsgegevens en-of stelselmatig monitoring van activiteiten van werknemers (bijvoorbeeld controle van e-mail en internetgebruik, GPS-systemen in (vracht)auto's van werknemers of cameratoezicht ten behoeve van diefstal- en fraudebestrijding). [3], [5], [7]
12. Locatiegegevens
Grootschalige verwerking en/of stelselmatige monitoring van locatiegegevens van of herleidbaar tot natuurlijke personen (bijvoorbeeld door (scan)auto's, navigatiesystemen, telefoons, of verwerking van locatiegegevens van reizigers in het openbaar vervoer). [3], [5]
13. Communicatiegegevens
Grootschalige verwerking en/of stelselmatige monitoring van communicatiegegevens inclusief metadata herleidbaar tot natuurlijke personen, tenzij en voor zover dit noodzakelijk is ter bescherming van de integriteit en de veiligheid van het netwerk en de dienst van de betrokken aanbieder, of het randapparaat van de eindgebruiker. [3], [5]

Wat is een DPIA?
Een PIA is een vragenlijst waarmee je de privacy risico's van je project in kaart brengt. Bij twijfel of een PIA verplicht is, kan het verstandig zijn om ertoe te besluiten er wel een uit te voeren, het kan nooit kwaad te weten waar de privacy risico's liggen binnen een project. Na het in kaart brengen van de risico's analyseer je de maatregelen die je genomen hebt om die risico's te beperken (bijvoorbeeld pseudonimiseren), als onderaan de streep blijkt dat er nog steeds sprake is van een hoog risico zul je terug moeten naar de tekentafel. Je mag niet beginnen met de verwerking voordat het risico voldoende beperkt is.

Kan MAAS voor mij een DPIA of PIA uitvoeren?
Het maken van een Data Privacy Impact Assessment (DPIA) is uw eigen verantwoordelijkheid als verwerkingsverantwoordelijke. Uiteraard zullen we u daarin ondersteunen door het leveren van informatie via de CIO en FG.

Voor het maken van een DPIA heb ik het verwerkingsregister van MAAS nodig. Kunnen jullie die delen?
Het verwerkingsregister zelf is bedoeld voor intern gebruik en om de Autoriteit Persoonsgegevens te kunnen informeren, en wordt dus niet met klanten gedeeld.
MAAS kan informatie die haar klanten kunnen gebruiken voor het uitvoeren van een Data Privacy Impact Assessment (DPIA) beschikbaar stellen via CIO en FG.

In welke gevallen moet ik een DPIA uitvoeren?
Als verantwoordelijke moet u een data protection impact assessment (DPIA) uitvoeren wanneer uw gegevensverwerking waarschijnlijk een hoog privacy risico oplevert. Dit moet u zelf bepalen. De volgende criteria kunnen u hierbij helpen. De Algemene verordening gegevensbescherming (AVG) geeft aan dat er in ieder geval een DPIA moet worden uitgevoerd als een organisatie:

- systematisch en uitgebreid persoonlijke aspecten evalueert gebaseerd op geautomatiseerde verwerking, waaronder profiling, en waarop besluiten worden gebaseerd die gevolgen hebben voor mensen;
- op grote schaal bijzondere persoonsgegevens verwerkt of wanneer er strafrechtelijke gegevens worden verwerkt ;
- op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

De Autoriteit Persoonsgegevens heeft een lijst opgesteld van soorten verwerkingen waarvoor het uitvoeren van een DPIA verplicht is vóórdat u met verwerken begint:
https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-ap-voor-een-verplichte-dpia-6667
Deze lijst is niet uitputtend. Het kan zijn dat uw verwerking niet op deze lijst staat. In dat geval zult u moeten beoordelen of uw verwerking een hoog privacy risico oplevert voor de betrokkenen. U kunt hierbij gebruik maken van de 9 criteria voor een DPIA die de Europese privacy toezichthouders hebben opgesteld. Als vuistregel geldt dat u een DPIA moet uitvoeren als uw verwerking aan 2 of meer van deze criteria voldoet.

Wanneer hoef ik geen DPIA uit te voeren?
U hoeft geen data protection impact assessment (PIA) uit te voeren wanneer uw gegevensverwerking:

- Waarschijnlijk geen hoog privacyrisico oplevert.
- Sterk lijkt op een andere gegevensverwerking waarvoor al een DPIA is uitgevoerd.
- Wordt geregeld door een andere Europese of nationale wet en er bij de totstandkoming van deze wet al een DPIA is uitgevoerd. Tenzij de privacytoezichthouder oordeelt dat er toch een DPIA nodig is.
- Op een lijst staat van verwerkingen waarvoor een DPIA niet verplicht is. De AVG geeft de privacytoezichthouder de mogelijkheid om zo'n lijst op te stellen, maar dit is niet verplicht. De AP heeft geen gebruik gemaakt van de mogelijkheid een dergelijke lijst op te stellen.

Moet ik alsnog een DPIA uitvoeren voor een bestaande verwerking?
Ja, soms moet u alsnog een data protection impact assessment (DPIA) uitvoeren voor een bestaande verwerking. Dat is als er iets verandert aan het risico van de gegevensverwerking. En de gegevensverwerking vervolgens (na de verandering) een hoog privacyrisico oplevert.
Geen DPIA nodig
U hoeft dus niet alsnog een DPIA uit te voeren als een van de volgende 3 situaties van toepassing is:

- uw gegevensverwerking levert waarschijnlijk géén hoog privacyrisico op;
- of u heeft voor deze verwerking al eens een voorafgaand onderzoek door de AP laten uitvoeren en de verwerking is in de tussentijd niet veranderd;

- of de risico's van de verwerking zijn niet veranderd.
    1. Verwerking verandert: Uw verwerking verandert bijvoorbeeld als u een nieuwe technologie gaat gebruiken. Of als u persoonsgegevens voor een ander doel gaat gebruiken. In deze situaties verandert uw gegevensverwerking feitelijk in een nieuwe gegevensverwerking. En dan kan een DPIA verplicht zijn.
    2. Risico verandert: Verandert het privacyrisico van uw verwerking? Dan kunt u ook verplicht zijn alsnog een DPIA uit te voeren. Risico's kunnen bijvoorbeeld veranderen omdat een onderdeel van het verwerkingsproces wijzigt. De technologische ontwikkelingen gaan snel, waardoor nieuwe kwetsbaarheden kunnen ontstaan.
    3. Omgeving verandert: Tot slot kunt u alsnog verplicht zijn een DPIA uit te voeren omdat de organisatie- of maatschappelijke context verandert. Bijvoorbeeld omdat de gevolgen van bepaalde geautomatiseerde beslissingen belangrijker zijn geworden of omdat er nieuwe categorieën mensen kwetsbaar worden voor discriminatie.

Hoe vaak periodieke DPIA?
Vanwege de hierboven genoemde veranderingen is het sowieso aan te raden om periodiek een DPIA uit te voeren. Ook als de gegevensverwerking zelf niet is veranderd. Bijvoorbeeld een keer per 3 jaar.

Wie moet een DPIA uitvoeren?
Als verantwoordelijke moet u ervoor zorgen dat er een data protection impact assessment (DPIA) wordt uitgevoerd. U moet hierbij, wanneer van toepassing, aan verschillende partijen advies vragen. U hoeft de DPIA niet zelf uit te voeren, dit kunt u ook door iemand anders binnen of buiten uw organisatie laten doen. U blijft wel eindverantwoordelijk.
Is er in uw organisatie een functionaris voor de gegevensbescherming (FG) aangewezen? Dan moet u de FG om advies vragen. U moet in het rapport over de DPIA opnemen wat de FG heeft geadviseerd en wat u daarmee heeft gedaan. De FG heeft ook als taak de uitvoering van de DPIA in de gaten te houden.
Advies bewerker
Voert een verwerker in opdracht van u de gegevensverwerking uit? Dan moet de bewerker u ondersteunen bij het uitvoeren van de DPIA en de informatie verstrekken die u nodig heeft.

Wie is verantwoordelijk voor de uitvoering?
Een veel voorkomende misvatting is dat de FG verantwoordelijk is voor het uitvoeren van een DPIA. Dat is niet het geval. Het uitvoeren van een DPIA is de verantwoordelijkheid van de verwerkingsverantwoordelijke (artikel 35, lid 2 AVG). De DPIA kan door iemand anders worden uitgevoerd, maar de verwerkingsverantwoordelijke blijft daarvoor eindverantwoordelijk.

Op welke manier moet ik een DPIA uitvoeren?
Er zijn verschillende methodes om een data protection impact assessment (DPIA) uit te voeren. U kunt er zelf een kiezen, als u maar aan de basisvereisten voldoet zoals die in de AVG staan beschreven.
Voorwaarden DPIA
De DPIA moet in ieder geval het volgende bevatten:

- Een systematische beschrijving van de beoogde gegevensverwerkingen en de doeleinden hiervan. Beroept u zich op een gerechtvaardigd belang als grondslag voor de verwerking? Neem dit dan ook op in de beschrijving.
- Een beoordeling van de noodzaak en de proportionaliteit van de verwerkingen. Dat houdt in: is het verwerken van persoonsgegevens op deze manier noodzakelijk op uw doel te bereiken? En is de inbreuk op de privacy van de betrokkenen (de mensen van wie u gegevens verwerkt) niet onevenredig in verhouding tot dit doel?
- Een beoordeling van de privacy risico’s voor de betrokkenen.
- De beoogde maatregelen om (1) de risico's aan te pakken (zoals waarborgen en veiligheidsmaatregelen) en (2) aan te tonen dat u aan de AVG voldoet.

Moet ik de DPIA publiceren?
U bent dit niet wettelijk verplicht. Maar het is wel aan te raden om uw data protection impact assessment (DPIA), of een deel hiervan, te publiceren.
Het publiceren van de DPIA kan het vertrouwen in uw gegevensverwerkingen bevorderen. Bovendien legt u hiermee verantwoording af en bent u transparant. Dit geldt vooral als de verwerking van invloed is op het algemeen publiek, zoals bij de overheid.

- Samenvatting. De gepubliceerde DPIA hoeft niet de hele beoordeling te bevatten. Er is wellicht informatie die u niet openbaar wilt maken, zoals informatie over beveiligingsrisico’s of concurrentiegevoelige informatie. U kunt dan volstaan met een samenvatting van de belangrijkste resultaten van de DPIA.
- Voorafgaande raadpleging. Let op: komt er uit de DPIA dat de verwerking een hoog risico oplevert als u geen risicobeperkende maatregelen neemt? Dan moet u een voorafgaande raadpleging aanvragen bij de Autoriteit Persoonsgegevens (AP). Hierbij moet u de DPIA aan de AP verstrekken.

Mag onder de AVG geen marketingcampagnes meer doen zonder vooraf een PIA (Privacy Impact Assessment) uit te voeren?

Dit is niet waar. Het uitvoeren van een Privacy Impact Assessment (PIA) wordt alleen verplicht voor verwerkingen met een hoog risico voor de betrokkenen. Dit zal zeker niet bij iedere campagne het geval zijn. Het wordt wél verplicht om te beoordelen of een PIA nodig is, door te signaleren controleren wat het risico van een verwerking (of serie verwerkingen) van persoonsgegevens inhoudt. Het versturen van een e-mailcampagne zal geen hoog risico voor betrokkenen inhouden. Dat kan anders zijn wanneer je gebruik maakt van een combinatie van locatiedata en het internetgedrag over meerdere websites. Ook het gebruik van een nieuwe technologie zoals beacons of RFID chips kunnen aanleiding geven tot een verplichte PIA.

40. AVG. Due diligence

Wat zegt de Autoriteit Persoonsgegevens over due diligence?
Geen actuele informatie,
https://autoriteitpersoonsgegevens.nl/nl/nieuws/verstrekken-van-personeelsgegevens-v%C3%B3%C3%B3r-overname-van-onderneming-bij-ontslag-%C2%A0

Overig:

- https://www.ploum.nl/due-diligence-avg-proof/
- https://www.valegis.com/news-posts/avg-en-ma-de-invloed-van-privacyregelgeving-op-de-overnamepraktijk/
- https://www.boelszanders.nl/publicatie/welke-invloed-avg-op-transactiepraktijk/

Mag de verkoper van een onderneming persoonsgegevens van werknemers zomaar aanleveren?
Voorafgaand aan de overname van een onderneming wordt tussen verkoper en potentiële koper onderling veel informatie uitgewisseld, waaronder ook persoonsgegevens van werknemers. Denk bijvoorbeeld aan het verstrekken van personeelsdossiers of het verstrekken van informatie over de arbeidsvoorwaarden. Ook bij een overname dient de de Algemene Verordening Gegevensbescherming ('AVG') nageleefd te worden. Interessant is daarom de vraag in hoeverre een due diligence onderzoek – in het kader van een overname – AVG-proof is. In deze bijdrage gaan we kort in op de belangrijkste gevolgen van de AVG ten aanzien van de overnamepraktijk.

De AVG en het due diligence onderzoek?
Een due diligence onderzoek heeft betrekking op de vermogenstoestand van een onderneming, inclusief mogelijke verborgen verliezen of te verwachten verliezen. Daarbij zullen mogelijk ook persoonsgegevens van werknemers worden onderzocht, zoals arbeidsovereenkomsten, salarisgegevens en andere afspraken met individuele werknemers. Een dergelijk onderzoek wordt meestal in opdracht van de potentiële koper uitgevoerd.
Onder de AVG kan een verkoper in het kader van een due diligence onderzoek niet zomaar persoonsgegevens van werknemers verstrekken aan potentiële kopers.

Grondslag van de verwerking?
De AVG bepaalt onder meer dat een verwerking – en dus ook verstrekking – van persoonsgegevens moet zijn gebaseerd op een rechtmatige grondslag. Kan dit niet, dan is het niet toegestaan om persoonsgegevens te verwerken. De verwerking kan in dit geval plaatsvinden op de grondslag 'gerechtvaardigd belang': de potentiële koper heeft immers een gerechtvaardigd belang om boekenonderzoek te doen en eventuele risico's te analyseren voordat hij besluit een onderneming over te nemen.

Doel van de verwerking?
Verder mogen persoonsgegevens slechts worden verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Het doel voor de verwerking van persoonsgegevens in het kader van een due diligence onderzoek betreft uiteraard het uitvoeren van een boekenonderzoek naar de mogelijk over te nemen onderneming. Vanuit arbeidsrechtelijk perspectief heeft de uitvoering van een due diligence specifiek betrekking op de arbeidsvoorwaarden, contractuele aanspraken, mogelijke claims van werknemers of derden (zoals een pensioenfonds) en het financieel beeld van de verkoper. Dit is uiteraard een gerechtvaardigd doel om informatie over werknemers te delen met een potentiële koper.

Proportionaliteit en subsidiariteit?
Nu de grondslag en het doel voor de verwerking zijn vastgesteld, is nog de vraag welke persoonsgegevens van werknemers precies mogen worden gedeeld in een due diligence. De verkoper dient steeds na te gaan of (I) de gegevensverwerking proportioneel is (staat de verwerking in verhouding tot het doel daarvan?) en of (II) de verwerking voldoet aan de eis van subsidiariteit (kan het doel ook op een minder vergaande manier worden bereikt?). Vuistregels daarbij zijn voor het bewaren van persoonsgegevens 'hoe korter, hoe beter' en voor de toegankelijkheid van persoonsgegevens 'hoe minder, hoe beter'. Bij de vraag of een due diligence onderzoek voldoet aan de AVG kan de volgende checklist door de verkoper gehanteerd worden:
Anonimiseer alle documenten (zoals een personeelslijst, overzicht van ziekteverzuim). Een koper hoeft immers niet te weten dat werknemer Jan of Piet langdurig ziek is: voldoende is om te weten dat er een langdurig ziektetraject loopt binnen de over te nemen onderneming.
Voorkom dat informatie herleidbaar is naar een specifieke werknemer, ondanks anonimisering. Als er maar één IT-manager is, en er wordt vastgelegd dat er een arbeidsconflict speelt met de IT-manager, is het eenvoudig om te achterhalen om welke werknemer het precies gaat. Het zou dan beter zijn om mee te delen dat er een arbeidsconflict speelt met iemand uit het managementteam of op de IT-afdeling.
Verstrek, indien mogelijk, modelarbeidsovereenkomsten aan de potentiële koper. Als dit niet mogelijk is, dienen namen, geboortedata, geslacht en andere persoonsgegevens van werknemers uit de arbeidsovereenkomst verwijderd te worden. Wij adviseren dit ook te doen bij contracten met zzp'ers. Let daarbij ook op het BTW-nummer, waar het BSN van de zzp'er in verwerkt zit.
Deel slechts de persoonsgegevens die relevant zijn voor een potentiële koper en slechts voor zover strikt noodzakelijk. Het is beter dat een koper tijdens het onderzoek vraagt om aanvullende informatie, dan dat een overvloed aan onnodige persoonsgegevens in de dataroom wordt geüpload. Indien een koper specifieke persoonsgegevens wil ontvangen, kan worden overlegd wat daar de noodzaak van is en hoe de privacy van de betrokken werknemers dan wordt gewaarborgd.
Bedenk hoe informatie op een minder vergaande manier kan worden gedeeld. Wellicht kan bijvoorbeeld de leeftijd van de werknemer in een overzicht worden opgenomen, in plaats van de geboortedatum. De potentiële koper krijgt zo alsnog een goed inzicht in de leeftijdsopbouw in de onderneming, zonder dat de geboortedatum direct naar een bepaalde werknemer leidt.
Werk met een dataroom waarin alle documenten goed beveiligd zijn, niet zomaar voor iedereen toegankelijk zijn en worden verwijderd na afloop van de due diligence.

Bedrijfsvoering AVG-compliant?
Belangrijk is de vraag of de over te nemen onderneming in de bedrijfsvoering 'AVG-compliant' is. Dit gelet op het risico op forse boetes en reputatieschade. Vragen die in het DD zeker gesteld moeten worden zijn bijvoorbeeld: Is er een verwerkingsregister? Zijn alle verwerkersovereenkomsten op orde? Is een functionaris gegevensbescherming verplicht en zo ja, is die er? Hoe is het niveau van de informatiebeveiliging?
De uitkomsten van het DD zijn uiteraard van belang in de onderhandelingen. Dat het al dan niet voldoen aan de AVG gevolgen heeft voor de koopprijs, ligt voor de hand. Ook heeft het invloed op het opnemen van garanties en/of vrijwaringen in het overnamecontract met betrekking tot AVG-compliance en IT-beveiliging.
Tijdens een DDO dient tegenwoordig als gevolg van de AVG ook aandacht te worden besteed aan de vraag in hoeverre de target privacy-compliant is. Om latere (financiële) tegenvallers te voorkomen kan het verstandig zijn om een "privacy" due diligence uit te voeren. Hierbij wordt gekeken of de target aan alle relevante privacy wetgeving voldoet, waaronder natuurlijk de AVG. Daarbij zijn vragen relevant zoals: hoe verzamelt, gebruikt, vernietigt, wist of slaat de target persoonsgegevens op? Hoe gaat de target om met datalekken? Is er een verwerkings- en datalekkenregister

bijgehouden? Zijn er datalekken geweest in het verleden? Heeft de target een functionaris voor gegevensbescherming aangesteld indien dit noodzakelijk is?
Voor deze compliance-check kan het verwerkingsregister van de target een goed uitgangspunt bieden. Hierin wordt immers bijgehouden wat voor soort persoonsgegevens de target verwerkt, voor welke doelen, op welke manier, wat de bewaartermijnen zijn, hoe de gegevens worden beveiligd, etc.

Gevolgen AVG voor Non Disclosure Agreement ("NDA")?
Voorafgaande aan een overname is het verstandig om in een geheimhoudingsverklaring (oftewel NDA), naast afspraken over geheimhouding, ook afspraken te maken over het naleven van privacy wetgeving zowel tijdens de onderhandeling als na de overname. Denk hierbij bijvoorbeeld aan afspraken over de opslag, teruggave en vernietiging van persoonsgegevens voor het geval de deal niet doorgaat of aan een verbod tot verstrekking van persoonsgegevens aan derde partijen alsmede dat de verzamelde persoonsgegevens uitsluitend ter evaluatie en beoordeling van de target worden gebruikt.
Maar ook indien deze afspraken niet worden vastgelegd, moeten partijen voldoen aan de AVG. Zowel koper als verkoper zijn te kwalificeren als verwerkingsverantwoordelijke en hebben ook zelfstandig de verplichting om de AVG na te leven.

Gevolgen AVG voor Share Purchase Agreement ("SPA")
Afhankelijk van wat uit het DDO blijkt met betrekking tot de mate waarin de target aan alle verplichtingen voortvloeiende uit de AVG voldoet, kan het verstandig zijn om hieromtrent het een en ander in de koopovereenkomst te regelen.
Mocht blijken dat de target nog niet helemaal "AVG-proof" is, kan het financiële risico van de koper door het opnemen van specifieke garanties of vrijwaringen worden beperkt.

41. AVG. Informatie verstrekken aan betrokkene

Wat zegt de AP over informatie aan betrokkene?
Recht op duidelijke informatie over wat u met hun persoonsgegevens doet. Onder de AVG moet u aan een aantal specifieke eisen voldoen.
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/rechten-van-betrokkenen#is-een-privacyverklaring-volgens-de-avg-verplicht-6253

Welke informatie moet u verstrekken aan de betrokkene?
Wanneer u de gegevens bij de betrokkene zelf verzamelt, moet u tenminste de volgende informatie verstrekken bij de verkrijging:

- uw identiteit en uw contactgegevens, of de contactgegevens van uw vertegenwoordiger;
- indien u een functionaris voor de gegevensbescherming hebt aangesteld, de contactgegevens van deze functionaris;
- de doelen waarvoor u persoonsgegevens verwerkt;
- de grondslag waarop u de verwerking baseert;
- wanneer u de verwerking baseert op de grondslag ‘gerechtvaardigd belang’: wat uw gerechtvaardigd belang is;
- de eventuele ontvangers of categorieën ontvangers van de gegevens;
- in geval van verstrekking aan derde landen:
  - of er een adequaatheidsbesluit van de Commissie bestaat,
  - of passende waarborgen zijn getroffen, welke dit zijn en of hier een kopie van kan worden verkregen, dan wel waar die waarborgen kunnen worden geraadpleegd;
- de bewaartermijn, of als dat niet mogelijk is de criteria voor het bepalen ervan;
- de rechten van de betrokkene;
- in het geval van toestemming, dat de betrokkene die toestemming altijd weer kan intrekken;
- dat de betrokkene het recht heeft een klacht in te dienen over uw verwerking bij de Autoriteit
  Persoonsgegevens;
- of het verwerken van persoonsgegevens een wettelijke verplichting is of noodzakelijk is voor de
  uitvoering of het aangaan van een overeenkomst, of de betrokkene verplicht is die gegevens te
  verstrekken en wat de gevolgen zijn van het niet verstrekken van die gegevens voor de betrokkene;
- in geval van geautomatiseerde besluitvorming, nuttige informatie over de onderliggende logica,
  het belang van de verwerking en de verwachte gevolgen van die verwerking voor de betrokkene.
- Verder moet alle andere informatie worden verstrekt die noodzakelijk is om tegenover de betrokkene een behoorlijke en transparante verwerking te waarborgen. U moet zelf bepalen welke aanvullende informatie naast deze verplichte elementen het eventueel zou betreffen.

42. AVG. Meerfactorauthenticatie

Wat zegt de Autoriteit Persoonsgegevens over meerfactorauthenticatie?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/beveiliging-van-persoonsgegevens#wat-is-meerfactorauthenticatie-6067

Wat is meerfactorauthenticatie?
Meerfactorauthenticatie is een vorm van toegangsbeveiliging waarbij de gebruiker zich met een combinatie van minimaal twee verschillende typen authenticatiefactoren moet authentiseren om toegang te krijgen tot een computer, besturingssysteem of applicatie. Denk aan de combinatie van het gebruik van een wachtwoord én een eenmalig te gebruiken paswoord of wachtwoord (token) per sms. Het Nationaal Cybersecurity Center heeft een factsheet over het gebruik van tweefactorauthenticatie:
https://www.nctv.nl/binaries/Factsheet%20gebruik%20tweefactorauthenticatie_tcm31-242994.pdf

Wanneer is meerfactorauthenticatie in ieder geval verplicht?
Indien bijzondere persoonsgegevens worden verwerkt, zoals gegevens over iemands gezondheid, strafrechtelijke gegevens, biometrische gegevens, gegevens over politieke of religieuze overtuigingen of seksueel gedrag, dan is het risico hoog. Dat is ook zo bij gegevens van gevoelige aard, zoals bijvoorbeeld inloggegevens, financiële gegevens of prestatiegegevens (denk aan functioneringsverslagen). Dan is meerfactorauthenticatie in ieder geval verplicht.

43. AVG. Onderzoek

Wat zegt de AP over onderzoek?
https://autoriteitpersoonsgegevens.nl/nl/nieuws/gedragscode-voor-verwerking-van-persoonsgegevens-bij-onderzoek-en-statistiek

Valt onderzoek onder de AVG?
Wanneer het een markt of medewerker onderzoek niet anoniem uitvoert is er sprake van verwerkingen van persoonsgegevens, daardoor valt het wél binnen de AVG. Het misverstand komt waarschijnlijk door de Telecommunicatiewet. Omdat marktonderzoek vaak niet voor commerciële, charitatieve of ideële doeleinden plaatsvindt kan het daarmee buiten de Telecommunicatiewet vallen. Dit heeft invloed op de regels voor e-mail en telemarketing.

Wanneer kan iets beschouwd worden als marktonderzoek?
De wetgever zegt over de Telecommunicatiewet het volgende: Onder marktonderzoek wordt in zijn algemeenheid verstaan: *"Iedere vorm van kwantitatief en/of kwalitatief onderzoek met gebruikmaking van statistische of andere wetenschappelijke methodes waarmee wordt beoogd om over doelgroepen of populaties uitspraken te doen op niet-individueel identificeerbaar niveau."*
Om te kunnen spreken over markt- en verkiezingsonderzoek mag er geen sprake zijn van een directe/rechtstreekse koppeling tussen de vergaarde informatie en verkoop of werving. Er is ook dan sprake van een directe koppeling van de verzamelde informatie met verkoop of werving, indien de verzamelde informatie (op een later tijdstip) wordt gebruikt om personen waarover informatie is verzameld te benaderen voor verkoop of werving.
Marktonderzoek is dus niet voor commerciële, charitatieve of ideële doeleinden en valt daarmee onder bepaalde voorwaarden buiten de Telecommunicatiewet. Voor 'puur' marktonderzoek via e-mail is toestemming dus niet nodig. Zolang deze gegevens niet worden gebruikt om rechtstreeks de betrokkene te benaderen met een aanbod, is er geen sprake van direct marketing en is de bepaling (artikel 11.7 Tw) niet van toepassing.
Maar wanneer het marktonderzoek ook een commerciële/upselling boodschap bevat valt het wel onder de bepaling en is toestemming wel een vereiste. Dit zijn marktonderzoeken waarin je een aanbod doet, oproept tot doneren of de organisatie promoot.

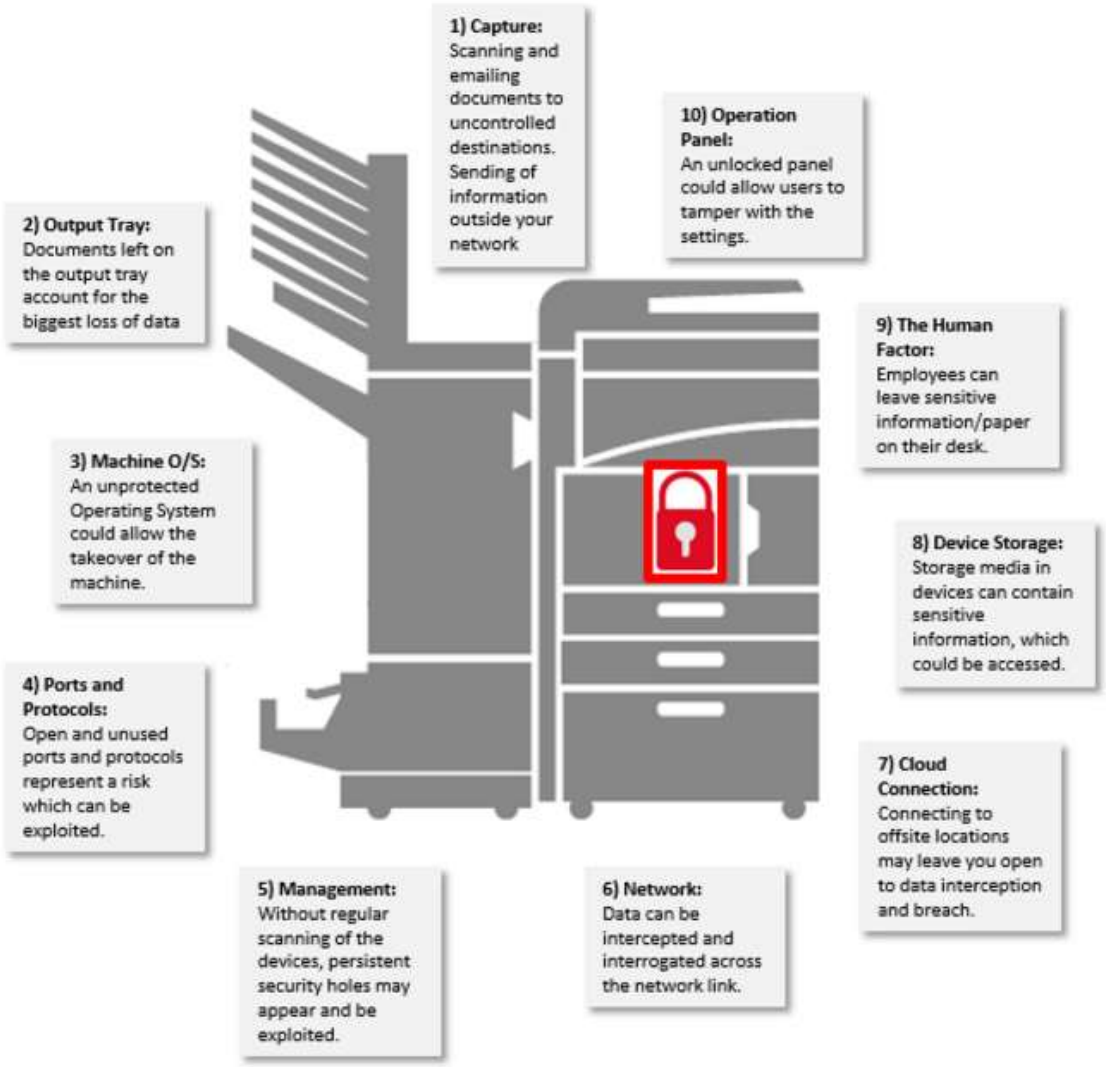
Gedragscodes?
https://www.moa.nl/codes-standards/gedragscodes.html
https://sharedpictures.moaweb.nl/images/MOAweb/Bestanden/pdf/AVG_Vragen28042018_inhoudsopgave_def.pdf

44. AVG. Printerpark

Wat zegt de AP over printers?
Geen specifieke info

Welk effect op printerpark door de AVG?
Tegenwoordig zijn printers en multifunctionals (MFP's) intelligente, via een netwerk verbonden, machines, die net zoals een pc een scherm, toetsenbord, harde schijf (die mogelijk gevoelige informatie kan opslaan) en besturingssysteem (OS) bevatten.
Toenemende cybercriminaliteit die direct gericht is op netwerkapparatuur, waaronder printers, is aangemerkt als een zwakke link in de verdediging tegen bedrijfsdiefstal en een kwaadaardige aanval.

Welke kwetsbaarheden van het printerpark?
Printerpark in hun algemene gegevensbescherming- en beveiligingsstrategie opnemen.
Kwetsbaarheden ten aanzien van de beveiliging van een MFP voor u geëvalueerd; welke kunnen worden verminderd of voorkomen door de beveiligingsmaatregelen (inclusief encryptie van MFP-harde schijven) die hieronder zijn beschreven te implementeren.
https://www.puntnlgroep.nl/veilige-outputomgeving/



45. Rechten. Controle over je data

Wat zegt de Autoriteit Persoonsgegevens over controle over je data?
Zie https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/controle-over-je-data

Hoe zit het met recht op inzage, correctie en verwijdering?
Iedereen mag aan een organisatie vragen of, en zo ja, welke gegevens deze organisatie van deze persoon heeft. Er mag alleen gevraagd worden naar gegevens van iemand zelf, niet naar gegevens van iemand anders. De mogelijkheid om van dit recht gebruik te maken wordt duidelijk en helder uitgelegd, zodat er geen drempel wordt opgeworpen om er gebruik van te maken.

Wat te doen als iemand vergeten wilt worden?
Dan zal diegene MAAS benaderen via mail of via contactformulier website. Je zult dan de vraag moeten loggen. Je zult dan alle informatie waar geen wettelijke bewaarplicht voor is (omdat gewerkt heeft voor je of ziek geweest is tijdens werk) moeten verwijderen. Ook als diegene eerder toestemming heeft gegeven om het te bewaren of jezelf in je statement hebt gezegd dat je het voor een langere tijd wilt bewaren. Daarvoor is het ook handig om een verwerkingsregister te hebben en te weten waar gegevens van die persoon kan staan. Vaak zal de persoon ook vragen welke gegevens je van hem of haar hebt staan; dan zal je daar een overzicht van moeten geven. Nog snel even gegevens verwijderen is in strijd met de AVG en wetgeving.

46. Rechten. Van betrokkenen

Wat zegt de Autoriteit Persoonsgegevens over rechten van betrokkene?
Zie https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/rechten-van-betrokkenen. FAQ's over de AVG-privacyrechten

Wat zijn de plichten als u de gegevens buiten de betrokkene om verkrijgt?
Wanneer u gegevens verzamelt buiten de betrokkene om, dan moet u in beginsel dezelfde informatie
verstrekken als wanneer u de gegevens van de betrokkene zelf heeft gekregen. Het enige dat u moet toevoegen is de bron waaruit de persoonsgegevens zijn verkregen. Als de bron van de informatie niet kan worden vastgesteld dient u algemene informatie over de herkomst te verstrekken.

Wanneer moet ik betrokkene opnieuw informeren?
Als u de persoonsgegevens voor andere doelen verder gaat verwerken, moet u de betrokkene opnieuw
informeren over dat nieuwe doel en opnieuw alle hierboven genoemde informatie verstrekken, behalve
voor zover de betrokkene al van die informatie op de hoogte is.

Wie is de betrokkene bij een overeenkomst met klanten?
In de context van MAAS zijn de betrokkenen uw contactgegevens om de overeenkomst te kunnen uitvoeren. Uw contactgegevens worden binnen de softwarepakketten van MAAS opgeslagen en verwerkt.

Wie is de betrokkene bij een arbeidsovereenkomst?
Als je kijkt naar de werkgever-werknemer verhouding is de werkgever de verantwoordelijke en de werknemer de betrokkene. De werkgever bepaalt als verantwoordelijke met welk doel bepaalde gegevens van de werknemer verwerkt worden.

Wat wijzigt er met de komst van de AVG ten aanzien van de betrokkene?
Met de introductie van de AVG worden de privacyrechten van de betrokkene verder versterkt en uitgebreid. Voor MAAS is het nieuwe 'recht op vergetelheid' belangrijk. Dat houdt in dat MAAS (onder bepaalde voorwaarden) de persoonsgegevens van de betrokkene dient te wissen wanneer de betrokkene daarom vraagt. Op de website van de Autoriteit Persoonsgegevens staat onder welke voorwaarden dit plaats dient te vinden.

47. Rechten. Dataportabiliteit

Wat zegt de Autoriteit Persoonsgegevens over het recht op dataportabiliteit. Het recht om persoonsgegevens over te dragen (NIEUW)?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/rechten-van-betrokkenen#wat-houdt-het-recht-op-dataportabiliteit-in-6345

48. Recht. Vergetelheid

Wat zegt de Autoriteit Persoonsgegevens over het recht op vergetelheid. Het recht om 'vergeten' te worden (NIEUW)?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/rechten-van-betrokkenen#wat-houdt-het-recht-op-vergetelheid-uit-de-avg-in-5976

Hoe maak ik gebruik van het vergeetrecht bij MAAS?
MAAS heeft een kort protocol waarin het vergeetrecht is geregeld.

Hoe werkt het protocol vergeetrecht bij MAAS?
Het vergeetrecht (ook wel bekend als *Het recht om vergeten te worden*, *The right to be forgotten* of *The right to erasure*) heeft betrekking op het verwijderen van persoonsgegevens en dat verdere verspreiding wordt tegengegaan. Het vergeetrecht heeft vooral betrekking op het verwijderen van persoonsgegevens uit zoekmachines. MAAS publiceert slechts op een beperkt aantal websites zelf content. Op deze websites worden zelden persoonsgegevens getoond. Mocht u er echter tegenaan lopen dat MAAS uw persoonsgegevens heeft gepubliceerd, en u wenst van het vergeetrecht gebruik te maken, dan kunt u dit bij MAAS aangeven. Neem dan contact met MAAS op via het contactformulier.
MAAS tracht uw verzoek zo spoedig mogelijk en in ieder geval binnen vier weken na uw aanvraag in behandeling te nemen.

Jurisprudentie vergeetrecht?
Verbod op het gebruik maken van een in het kader van een arbeidsconflict opgesteld rapport is afgewezen, art. 17 AVG wissen van gegevens is geen absoluut recht | ECLI:NL:RBAMS:2018:7398, r.o. 4.8
https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2018:7398

Hoe heeft MAAS het recht op inzage geregeld?
MAAS heeft een protocol waarin het recht op inzage is geregeld: Privacy reglement

49. Rechten. Inzage

Wat zegt de Autoriteit Persoonsgegevens over het recht op inzage. Dat is het recht van mensen om de persoonsgegevens die u van hen verwerkt in te zien?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/rechten-van-betrokkenen#wat-houdt-het-recht-op-inzage-in-6346

Hoe werkt het protocol inzagerecht bij MAAS?
MAAS slaat zeer beperkt persoonsgegevens op. Welke data MAAS opslaat staat in het Privacy beleid MAAS. Wenst u te weten welke gegevens MAAS van u persoonlijk bezit, dan kunt u dit bij MAAS opvragen. Voorwaarde is wel dat u 16 jaar of ouder bent en kunt aantonen dat de gegevens die u wilt inzien aan u toebehoren, of dat u de wettelijke vertegenwoordiger bent. Wenst u bijvoorbeeld te weten of wij uw e-mailadres hebben opgeslagen, dan dient u altijd een controlevraag van MAAS via dit e-mailadres bij ons te bevestigen. Ook kan het zijn dat u een kopie van uw identificatiebewijs moet sturen, waarna MAAS altijd een dubbele controle zal uitvoeren om uw identiteit vast te stellen. Als uw identiteit onomstotelijk is bevestigd, gaat MAAS het volgende voor u na:

- of u bij MAAS bekend bent, zo ja:
- welke gegevens wij van u bezitten;
  wat het doel is van het gebruik;
  aan wie de gegevens eventueel zijn verstrekt;
- wat de herkomst is van de gegevens, als deze bekend is.

Mits u dit wenst, en dit technisch haalbaar is, dan kunnen wij de gegevens voor u verwijderen. Wenst u gebruik te maken van Het recht op inzage, neem dan contact met MAAS op via het contactformulier.
MAAS tracht uw verzoek zo spoedig mogelijk en in ieder geval binnen vier weken na uw aanvraag in behandeling te nemen.

Jurisprudentie over inzage:

- Het recht op inzage betekent niet automatisch recht op kopieën van stukken waarin persoonsgegevens voorkomen, maar wel recht op een volledig en begrijpelijk overzicht van de verwerkte persoonsgegevens | ECLI:NL:RBNHO:2019:4283
  https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBNHO:2019:4283
- Werknemer heeft recht op inzage in het personeelsdossier | ECLI:NL:RBMNE:2018:3624
- Verwerking door onderzoeksbureau van persoonsgegevens werknemer rechtmatig wegens gerechtvaardigd belang werkgever dat inbreuk op privacy rechtvaardigde; verzoek tot inzage afgewezen wegens gebrek aan belang | ECLI:NL:RBAMS:2019:2166
  https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2019:2166

50. Rechten. Rectificatie en aanvulling

Wat zegt de AP over het recht om bezwaar te maken tegen de gegevensverwerking?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/rechten-van-betrokkenen#wat-houdt-het-recht-op-rectificatie-in-6347

Jurisprudentie?
Er is nog weinig rechtspraak over het equivalente 'recht op rectificatie' van artikel 16 AVG. Hoewel in artikel 16 AVG – anders dan in artikel 36 Wbp – niet wordt gesproken over 'feitelijk onjuist', maar over 'onjuist', ligt het niet voor de hand dat in het vervolg ook indrukken, meningen, onderzoeksresultaten en conclusies in (bestuurlijke) documenten met een beroep op artikel 16 AVG zullen kunnen worden gecorrigeerd.
Artikel 16 AVG bevat overigens geen regeling voor de situatie dat in een gegevensdrager geen wijzigingen kunnen worden aangebracht. Dat is jammer, want het komt in de praktijk voor dat gegevensdragers niet gewijzigd kunnen worden. Dat speelt evident bij de blockchain, die juist is gebaseerd op het uitgangspunt dat er niets kan worden gewijzigd.

51. Rechten. Op beperking van de verwerking

Wat zegt de AP over het recht op beperking van de verwerking: Het recht om minder gegevens te laten verwerken?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/rechten-van-betrokkenen#wat-houdt-het-recht-op-beperking-van-de-verwerking-in-6348

52. Rechten. Op een menselijke blik bij besluiten

Wat zegt de AP over het recht met betrekking tot geautomatiseerde besluitvorming en profilering. Oftewel: het recht op een menselijke blik bij besluiten?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/rechten-van-betrokkenen#wat-houdt-het-recht-op-een-menselijke-blik-bij-besluiten-in-6371

53. Rechten. Om bezwaar te maken tegen de gegevensverwerking

Wat zegt de AP over het recht op rectificatie en aanvulling. Het recht om de persoonsgegevens die u verwerkt te wijzigen?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/rechten-van-betrokkenen#wat-houdt-het-recht-van-bezwaar-in-6349

54. MAAS. Maatregelen voor de AVG

Zijn MAAS medewerkers op de hoogte van de AVG?
MAAS medewerkers worden incidenteel getraind op het gebied van informatiebeveiliging en er wordt periodiek voorlichting verstrekt.
Er wordt niet eenmaal per kwartaal bij wijze van een steekproef gecontroleerd of MAAS medewerkers op de hoogte zijn van de huidige regelgeving en hier ook naar handelen.

Wordt MAAS getoetst op de AVG?
Ja, in het certificeringstraject voor het managementsysteem wordt de regelgeving uit de AVG ook meegenomen. MAAS wordt jaarlijks voor ISO9001:2015; ISO14001:2015 en ISO45001:2018 geaudit.

Heeft MAAS procedures voor het geval van een gegevenslek?
Vanuit de Algemene Verordening Gegevensbescherming (en al langer vanuit vroegere Wet bescherming persoonsgegevens) bestaat er een meldplicht datalekken. Op basis daarvan beschikt MAAS over een procedure die voorschrijft hoe te handelen in het geval van een gegevenslek. Alle MAAS medewerkers zijn op de hoogte van deze procedure.

Hoe beveiligt MAAS mijn data?
Nog niet van toepassing: Daarvoor maakt MAAS gebruik van encryptie. Voor elektronisch transport maakt MAAS gebruik van encryptie op basis van SSL. Voor het fysiek transporteren van data maken wij gebruik van geëncrypteerde USB-sticks. Daarnaast zijn alle PC's en laptops binnen MAAS voorzien van encryptie.

Hoe kan MAAS ons helpen te handelen in overeenstemming met de AVG?
MAAS is in 2017 gestart met het voorbereiden op de AVG en zorgt ervoor dat zowel de organisatie als de software voldoet aan de wetgeving. Wanneer u hierover vragen heeft dan kunt u deze altijd stellen door het sturen van een e-mail of door ons te bellen via het algemene telefoonnummer.

Werkt MAAS volgens het principe 'privacy by design'?
Nog niet van toepassing: Bij MAAS is privacy by design al sinds … de standaard. Eind …heeft MAAS alle systemen geanalyseerd en alle data verwijderd die niet strikt noodzakelijk was voor onze dienstverlening en/of een wettelijke bewaarplicht kenden. Vanaf dat moment slaat MAAS niet meer data op dan strikt noodzakelijk is.

55. MAAS. Medewerkers en de AVG

Waar vind ik als MAAS medewerker de MAAS informatie over de AVG?
Zie http://intranet.maas.nl/ onder het kopje Gegevensbescherming.

Hoe ga ik als MAAS medewerker zorgvuldig om met persoonsgegevens?
Het is belangrijk dat we allemaal zorgvuldig omgaan met persoonsgegevens. De belangrijkste tips:

- Verzamel en bewaar fysiek en digitaal geen informatie over (potentiële) medewerkers en of klantdata op je bureau, bureaublad, in je eigen Outlook omgeving, in je tas of in je leaseauto.
- Schoon (regelmatig) je e-mailbox en persoonlijke schijf op en verwijder klant- en of medewerkersgegevens.
- Verwerk je gegevens over medewerkers en/of klanten? Stem met je leidinggevende en je collega's af welke mogelijke AVG acties uitgevoerd dienen te worden en hoe je voortaan deze gegevens zorgvuldig verwerken.
- Heb je een nieuwe klant? Stem met je leidinggevende af of er sprake is van verwerking van data. Het is mogelijk dat er een Verwerkingsovereenkomst moet komen.

Wat is een datalek en hoe ga ik hier als medewerker mee om?
Een 'datalek' is er als vrijgekomen persoonsgegevens blootgesteld worden of in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Een datalek kan digitaal plaatsvinden (zoals uitgelekte computerbestanden met persoonsgegevens) en fysiek (zoals een gestolen geprinte klantenlijst). Voorbeelden:

- e-mail met persoonsgegevens verzonden naar verkeerde adressen
- gestolen laptop
- persoonsgegevens bij verkeerde klant getoond in klantportaal
- persoonsgegevens bij het oud papier geplaatst
- verloren usb-stick met persoonsgegevens
- persoonsgegevens per ongeluk gepubliceerd
- verloren bedrijfstelefoon
- cyberaanvallen

Heb je (een vermoeden van) een datalek?

A. Meld dit direct bij je leidinggevende en stuur een mail naar: fg@maas.nl.
B. De melding wordt opgepakt en wanneer jouw hulp nodig is, wordt er contact met je opgenomen.

Wat zijn de rechten van betrokkenen en hoe ga ik hiermee om?
Onder de AVG worden de privacyrechten van personen versterkt en uitgebreid. Om te kunnen voldoen aan de verzoeken van betrokkenen heeft MAAS de systemen, processen en interne organisatie op deze rechten ingericht.
In de AVG heeft een betrokkene (persoon) meerdere rechten waar hij of zij gebruik van mag maken:

- Recht op uitleg
- Recht op vergetelheid. Het recht om 'vergeten' te worden
- Recht op dataportabiliteit. Recht om je persoonsgegevens over te dragen
- Recht op inzage. Recht om je persoonsgegevens die organisaties verwerken in te zien
- Recht op rectificatie. Recht om je persoonsgegevens die organisaties verwerken te laten aanpassen of aanvullen
- Recht op beperking van de verwerking. Recht om organisaties te vragen om het gebruik van je persoonsgegevens te beperken
- Recht op bezwaar. Recht om bezwaar te maken tegen de gegevensverwerking.

Instructie wanneer je een van bovenstaande verzoeken krijgt van betrokkenen:

A. Ga nooit zelf aan de slag met een verzoek. Geef aan dat wij er op terug komen bij hem of haar.
B. Meld dit direct bij je leidinggevende en stuur een mail naar: fg@maas.nl.
C. De melding wordt opgepakt en wanneer jouw hulp nodig is, wordt er contact met je opgenomen.

56. MAAS. One Coffe Connect (applicatie)

Heeft MAAS een contract met de leverancier van One Coffee Connect?
Ja, betreft de Amazon Webservice Hosted applicatie Kitchen Connect. Dossier in beheer bij Inkoop.

Is er een due diligence/ risicobeoordeling beschikbaar voor het geval de veilige status van de verwerking van persoonsgegevens via Welbilt KitchenConnect/ One Coffee Connect in twijfel wordt getrokken?
Ja, opvragen bij de Functionaris Gegevensbescherming.

Waarom is een due diligence/ risicobeoordeling voor OCC vereist?
Tot nu toe heeft de Europese Commissie voor slechts 12 landen een adequaatheidsbesluit afgegeven en het adequaatheidsbesluit voor de VS is nu tot twee keer toe ongeldig verklaard. Het Hof van Justitie van de Europese Unie (Hof) verklaarde namelijk 16 juli 2020 het EU-VS-privacyschild met onmiddellijke ingang ongeldig (Schrems II). Wel bevestigde het de geldigheid van Standard Contractual Clauses (SCC's), maar beperkte het effectief de situaties waarin de SCC's nog steeds kunnen worden vertrouwd en benadrukte het de (aanvullende) verplichtingen voor het gebruik ervan.

De verwerkingsverantwoordelijke moet een verwerkersovereenkomst beoordelen en is, als zij deze vrijelijk accepteert en gebruik maakt van de aangeboden dienst, er volledig verantwoordelijk voor dat deze voldoet aan de AVG. Door verwerker voorgestelde wijzigingen moeten telkens aan de verwerkingsverantwoordelijke worden voorgelegd en door hem worden goedgekeurd. Vereist is een constante monitoring die kan leiden tot (nood) opschortings- en beëindigingsverplichtingen onder de SCC als het derde land niet (meer) een niveau van gegevensbescherming biedt dat in wezen gelijkwaardig is aan dat gegarandeerd onder de AVG. Het gebruik van SCC's vereist daarom aanvullende maatregelen en onderhoud.
In de SCC:

- Is MAAS de data exporter en customer conform de hoofdovereenkomst. In deze hoofdovereenkomst is MAAS International B.V. gevestigd in Nederland en valt onder de AVG jurisdictie van de Nederlandse Autoriteit Persoonsgegevens. Bij een data breach zal MAAS dus melding moeten doen bij de AP;
- Is aangegeven dat de data exporter gevestigd is in Zweden. Bij een data breach zal CREM een melding moeten doen bij de Swedish Authority for Privacy Protection/ Integritetsskyddsmyndigheten (IMY);
- Is de data importer gevestigd in de VS. Er is momenteel geen EU adequaatheidsbesluit voor de VS.

MAAS heeft in november 2020 en vervolgens in januari 2021 in lijn met de aanbevelingen van de European Data Protection Board, een aanvulling op de SCC gevraagd. Deze aanvulling (Amendment no 1) is 14 januari 2021 opgesteld door Welbilt (CREM).
De AP eist dat MAAS als verwerkingsverantwoordelijke expliciet kan aantonen dat een specifiek gegevensverwerking, in dit geval die van Welbilt KitchenConnect/ One Coffee Connect, de AVG naleeft. Hieronder daarom de gedocumenteerde due diligence / risicobeoordeling van de afspraken tussen MAAS en Welbilt (CREM). Deze due diligence/ risicobeoordeling is daarmee beschikbaar voor het geval de veilige status van de verwerking van persoonsgegevens via Welbilt KitchenConnect/ One Coffee Connect in twijfel wordt getrokken.
Verwerkt MAAS persoonsgegevens in opdracht van een klant en dient er daarom een verwerkersovereenkomst tussen beide partijen te worden aangegaan?

Bij het bepalen of een verwerkersovereenkomst benodigd is bij het delen van persoonsgegevens wordt door de Autoriteit Persoonsgegevens (AP) gekeken naar de rolverdeling tussen de partijen. Het bedrijf wat het doel en de middelen van het gebruik van de persoonsgegevens bepaalt is de verwerkingsverantwoordelijke. Bij een contract voor de warme drankenvoorziening verwerken zowel MAAS als de klant persoonsgegevens van elkaars medewerkers, er is echter geen Verwerkingsovereenkomst nodig, omdat beide partijen zelfstandig verwerkingsverantwoordelijke zijn.

- MAAS heeft contactgegevens nodig om de diensten te kunnen uitvoeren en te factureren. De overeenkomst zelf is niet gericht zijn op het verwerken van persoonsgegevens, maar heeft een ander doel: warme dranken voorziening voor klant. MAAS bepaalt doel en middelen, AVG grondslag is uitvoering overeenkomst. MAAS meldt een eventueel datalek uit de eigen organisatie (IT, papier) van persoonsgegevens eigen medewerkers, klanten en contractors/leveranciers zelfstandig aan de Autoriteit Persoonsgegevens.
- Klant heeft contactgegevens nodig om diensten te kunnen afnemen en om facturen te kunnen betalen. De overeenkomst zelf is niet gericht zijn op het verwerken van persoonsgegevens, maar heeft een ander doel: koffievoorziening door MAAS. Klant bepaalt doel en middelen, AVG grondslag is uitvoering overeenkomst. Klant meldt datalek uit de eigen organisatie (IT, papier) van persoonsgegevens van eigen medewerkers, cliënten en contractors/leveranciers zelfstandig aan de Autoriteit Persoonsgegevens.

Op welke manier komen bij OCC personeelsgegevens wel om de hoek kijken en dus een verwerkersovereenkomst?

Bij OCC bestaat de verwerking van persoonsgegevens uit het aanbieden van software door MAAS aan de klanten, namelijk een (AWS) Hosted applicatie. De klant voert persoonsgegevens (emailadressen) in dit pakket in. Wanneer een klant persoonsgegevens in de OCC applicatie aanmaakt, is MAAS automatisch een verwerker in de zin van de AVG. Deze MAAS dienst wordt specifiek ingehuurd voor de opslag van data, maar de verwerkingsverantwoordelijke klant bepaalt welke gegevens worden opgeslagen en voor hoe lang. In dat geval in de verwerkersovereenkomst vanuit de klant dus specifiek alleen OCC verwerking aangeven. Bij een datalek in OCC meldt MAAS dit aan de klant. Klant meldt datalek OCC vervolgens aan de Autoriteit Persoonsgegevens.

Wat is vereist bij een (onverhoopt) datalek in OCC?

1. Mocht heel OCC een datalek hebben (bijvoorbeeld hack), dan dient MAAS alle gebruikers (klanten) te informeren. Iedere klant dient zelfstandig het datalek te melden bij de AP.
2. Het is niet zo dat MAAS als verwerker één melding mag doen namens alle (verwerkingsverantwoordelijke) klanten. MAAS zou dan namens elke verwerkingsverantwoordelijke een aparte datalekmelding bij de AP moeten doen en elke datalekmelding op naam van de betreffende verwerkingsverantwoordelijke moeten doen https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken.
3. Conform de MAAS contracten met Welbilt is MAAS controller en zal dus bij een datalek ook zelf een melding aan de AP moeten doen.

57. MAAS. One Coffee Connect (gebruiksprotocol)

Wat zegt de Autoriteit Persoonsgegevens over de gebruiksprotocol?
Geen info.

Waarom heeft MAAS een gebruiksprotocol voor One Coffee Connect?
Met OCC faciliteert MAAS een ICT oplossing/platform aan haar klanten om zonder goedkeuring van MAAS en zonder toezicht van MAAS berichten te plaatsen die in strijd zijn met de AVG waar MAAS aansprakelijk voor kan worden gehouden door betrokkenen.
MAAS is verplicht de AVG na te leven en vindt het belangrijk dat de privacy rechten van ieder individu worden gerespecteerd. Daarnaast wil MAAS is dat er respectvol wordt omgegaan met de communicatie die getoond wordt op de displays van de koffiemachines. Zo willen we voorkomen dat er communicatie op de displays gepubliceerd wordt welke de privacy rechten van individuen schenden en/of foutief en/of onnauwkeurig en/of krenkend en/of vulgair en/of tot haat aanzet en/of obsceen en/of beledigend is voor een groep mensen wegens hun ras, godsdienst of levensovertuiging of hun hetero/homoseksuele geaardheid en/of bedreigend en/of anderszins in strijd met de wet is dan wel iemand anders eer en/of goede naam aantast. Daarom heeft MAAS een “Gebruikersprotocol – voorwaarden plaatsen berichten” opgesteld waar de afnemer van de applicatie One Coffee Connect zich aan dient te houden. Afnemer, Key-User en Gebruikers krijgen alleen toegang tot de displays van de automaten indien Afnemer schriftelijk akkoord is gegaan met dit “Gebruikersprotocol – voorwaarden plaatsen berichten”.
Het Gebruikersprotocol biedt MAAS geen volledige bescherming tegen misbruik van OCC door klanten. Legal Counsel heeft zo goed als mogelijk de risico’s voor MAAS proberen te beperken. Als MAAS betere bescherming wil dan moet OCC (technisch gezien) anders worden ingericht.

Waarom heeft MAAS een boeteclausule opgenomen in het gebruiksprotocol voor One Coffee Connect?
Legal Counsel heeft een boete in het Gebruikersprotocol OCC opgenomen omdat met een boete MAAS de klanten die zich niet houden aan het Gebruikersprotocol OCC direct kan dwingen om het Gebruikersprotocol OCC toch na te leven en de overtreding per direct te beëindigen. Naast de boete kan MAAS ook de geleden schade op de klant verhalen. Boetes zijn zeer gebruikelijk in de praktijk. Kijk alleen al maar de contracten die MAAS heeft met haar klanten waarin op overtreding van de geheimhoudingsplicht een boete staat. Indien MAAS niet kiest voor een boete, wat Legal Counsel als buitengewoon onverstandig kwalificeert, dan dient MAAS de gebruikelijke juridische weg te bewandelen van ingebrekestelling, redelijke termijn en eventueel een gang naar de rechter, maar in de tussentijd gaat de klant gewoon verder met overtreding van het Gebruikersprotocol OCC en de ellende op het gebied van de AVG neemt alleen maar toe.

Verwerkt MAAS bij OCC persoonsgegevens in opdracht van een klant en dient er daarom een verwerkersovereenkomst tussen beide partijen te worden aangegaan?
Bij het bepalen of een verwerkersovereenkomst benodigd is bij het delen van persoonsgegevens wordt door de Autoriteit Persoonsgegevens (AP) gekeken naar de rolverdeling tussen de partijen. Het bedrijf wat het doel en de middelen van het gebruik van de persoonsgegevens bepaalt is de verwerkingsverantwoordelijke. Bij een contract voor de warme drankenvoorziening verwerken zowel MAAS als de klant persoonsgegevens van elkaars medewerkers, er is echter geen Verwerkingsovereenkomst nodig, omdat beide partijen zelfstandig verwerkingsverantwoordelijke zijn.

- MAAS heeft contactgegevens nodig om de diensten te kunnen uitvoeren en te factureren. De overeenkomst zelf is niet gericht zijn op het verwerken van persoonsgegevens, maar

heeft een ander doel: warme dranken voorziening voor klant. MAAS bepaalt doel en middelen, AVG grondslag is uitvoering overeenkomst. MAAS meldt een eventueel datalek uit de eigen organisatie (IT, papier) van persoonsgegevens eigen medewerkers, klanten en contractors/ leveranciers zelfstandig aan de Autoriteit Persoonsgegevens.
- Klant heeft contactgegevens nodig om diensten te kunnen afnemen en om facturen te kunnen betalen. De overeenkomst zelf is niet gericht zijn op het verwerken van persoonsgegevens, maar heeft een ander doel: koffievoorziening door MAAS. Klant bepaalt doel en middelen, AVG grondslag is uitvoering overeenkomst. Klant meldt datalek uit de eigen organisatie (IT, papier) van persoonsgegevens van eigen medewerkers, cliënten en contractors/leveranciers zelfstandig aan de Autoriteit Persoonsgegevens.

Op welke manier komen bij OCC personeelsgegevens wel om de hoek kijken en dus een verwerkersovereenkomst?
Bij OCC bestaat de verwerking van persoonsgegevens uit het aanbieden van software door MAAS aan de klanten, namelijk een Amazon Web Services (AWS) Hosted applicatie. De klant voert persoonsgegevens (emailadressen) in dit pakket in. Wanneer een klant persoonsgegevens in de OCC applicatie aanmaakt, is MAAS automatisch een verwerker in de zin van de AVG. Deze MAAS dienst wordt specifiek ingehuurd voor de opslag van data, maar de verwerkingsverantwoordelijke klant bepaalt welke gegevens worden opgeslagen en voor hoe lang. In dat geval in de verwerkersovereenkomst vanuit de klant dus specifiek alleen OCC verwerking aangeven. Bij een datalek in OCC meldt MAAS dit aan de klant. Klant meldt datalek OCC vervolgens aan de Autoriteit Persoonsgegevens.

Wat is vereist bij een (onverhoopt) datalek in OCC?
1. Mocht heel OCC een datalek hebben (bijvoorbeeld hack), dan dient MAAS alle gebruikers (klanten) te informeren. Iedere klant dient zelfstandig het datalek te melden bij de AP.
2. Het is niet zo dat MAAS als verwerker één melding mag doen namens alle (verwerkingsverantwoordelijke) klanten. MAAS zou dan namens elke verwerkingsverantwoordelijke een aparte datalekmelding bij de AP moeten doen en elke datalekmelding op naam van de betreffende verwerkingsverantwoordelijke moeten doen https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken
3. Conform de MAAS contracten met Welbilt is MAAS controller en zal dus bij een datalek ook zelf een melding aan de AP moeten doen.

Waarom biedt het gebruikersprotocol geen bescherming voor overtreding van AVG door gebruikers en wat is daar eventueel voor nodig?
Het Gebruikersprotocol biedt MAAS geen volledige bescherming tegen misbruik van OCC door klanten, omdat hiervoor meer nodig is.

Wat is technisch nodig om wel betere bescherming te krijgen?
Een set van verschillende maatregelen die elkaar aanvullen en versterken en die klant, MAAS en applicatieleverancier/ beheerder regelmatig moet controleren en waar nodig moet bijstellen (plan-do-check-act). Wat passend is hangt af van:
- Verwerkingsverantwoordelijke. De klant organisatie en van de kwetsbare onderdelen die de klant heeft geïnventariseerd.
- Verwerker (contract met klant) & verwerkingsverantwoordelijke (contract met leverancier OCC). MAAS organisatie en de kwetsbare onderdelen die de MAAS heeft geïnventariseerd.
- Subverwerker.

Minimaal de volgende maatregelen:

1) Hoe zien de informatiestromen eruit?
2) Waar zitten de kritieke bedrijfsprocessen?
3) Welke persoonsgegevens worden allemaal verwerkt?
4) Op welke plekken staan die opgeslagen?
5) Welke zijn het meest gevoelig?
6) Welke systemen zijn er?
7) Is er een functionaliteit of software aanwezig die niet (meer) nodig is?
8) Welke medewerkers hebben er allemaal toegang tot welke persoonsgegevens?
9) Hebben ze die toegang ook echt nodig voor hun functie?
10) Wat kan er misgaan? En welke risico's levert dat op? Denk aan inbraak, phishing, brand, kwijtraken van mobiele apparaten.

Hoe gebeurt het constateren van een overtreding van AVG bij OOC, hoe is MAAS dan in staat een boete op te leggen en waarom dat sneller zou werken dan een notificatie waarin we deze overtreding constateren en duidelijk maken dat hier boetes aan zitten als niet binnen 24 uur navolging aan onze instructies wordt gegeven?
Constateren zal gebeuren tijdens monitoren van OCC door MAAS medewerkers. *MAAS behoudt zich het recht voor berichten te verwijderen en hier zo nodig melding/aangifte van te doen van bij de politie.*
MAAS moet zich als verwerker zich volledig houden aan de instructies die MAAS krijgt van de klant verwerkingsverantwoordelijke voor het verwerken van de persoonsgegevens. Tenzij deze instructies in strijd zijn met de wet. Volgt MAAS de instructies van de klant niet? Dan beschouwt de AVG MAAS als verwerkingsverantwoordelijke met bijbehorende verplichtingen. Klant heeft als verwerkingsverantwoordelijke de plicht om het datalek te melden aan de Autoriteit Persoonsgegevens.

58. MAAS. Privacy verklaring

Wat zegt de autoriteit Persoonsgegevens over Privacy verklaring?

- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/rechten-van-betrokkenen#hoe-stelt-u-een-privacyverklaring-op-6255
- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/digitale-televisie-en-smart-tvs?qa=privacyverklaring&scrollto=1

Moet ik een privacy statement hebben op de website?
Een privacy statement is wettelijk verplicht voor elke website die persoonsgegevens van bezoekers gebruikt. U moet in het statement aangeven welke privacygevoelige gegevens u verzamelt en met welk doel. Een privacy statement moet voor klanten makkelijk te vinden. Als klanten op uw website via een digitaal bestelproces producten kunnen bestellen, dan is sterk aan te raden om het privacy statement (naast uw algemene voorwaarden) een “af te vinken” onderdeel van dit proces te laten zijn.

Welke informatie (in begrijpelijke taal!) moet het privacy statement minimaal bevatten?
Het privacy statement moet minimaal de volgende informatie bevatten:

- Identiteit en contactinformatie van de verwerkingsverantwoordelijke (bedrijfsgegevens contactgegevens in verband met inzage- en correctie recht alsmede het recht om vergeten te worden);
- Doel (bijv. contact opnemen, producten leveren etc.) en wettelijke basis voor de verwerking: welke gegevens verzameld worden;
- De legitieme belangen van de verwerkingsverantwoordelijke (als deze van toepassing is)
- Eventuele ontvangers (of categorieën van ontvangers) van de persoonsgegevens (bijvoorbeeld eventuele verwerkers)
- Informatie omtrent het doorsturen van de persoonsgegevens naar een derde land (buiten EU), indien van toepassing, waar u de gegevens opslaat (in Nederland of elders);
- De bewaartermijn, of de criteria waarmee de bewaartermijn bepaald wordt, dus hoe lang u de gegevens wilt bewaren;
- De betrokkene dient gewezen te worden op de rechten die hij heeft
- De betrokkene dient gewezen te worden op het recht om zijn toestemming voor de verwerking in te trekken
- De betrokkene dient gewezen te worden op zijn recht om een klacht in te dienen bij de toezichthouder
- Als gebruik wordt gemaakt van geautomatiseerde besluitvorming dient dit vermeld te worden
- uitleg over inzage en correctie recht van de opgegeven privacy gegevens en de verwijdering daarvan (het recht om vergeten te worden);
- op welke wijze u de gegevens beveiligt;

59. MAAS. Register van verwerkingen

Wat zegt de Autoriteit Persoonsgegevens over het register van verwerkingsactiviteiten?

- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/verantwoordingsplicht#ben-ik-verplicht-om-een-register-van-verwerkingsactiviteiten-op-te-stellen-6101

Benchmark?

De tool is oorspronkelijk gemaakt voor het registreren van meldingen aan de Autoriteit Persoonsgegevens (AP). In het register staan alle processen in het kader waarvan verwerkingen van persoonsgegevens plaatsvinden binnen het ministerie. Je kunt daarbij denken aan bijvoorbeeld een subsidie- of belastingadministratie, maar ook aan cameratoezicht. In al die gevallen worden persoonsgegevens verwerkt (zoals het opslaan, bewaren of verspreiden). Dat register is openbaar. Elke melding bevat een korte beschrijving van de soorten gegevens die worden verwerkt, waarvoor die gegevens zijn verzameld, wat er met de gegevens wordt gedaan en wie er verantwoordelijk is voor de verwerking. De tool wordt beheerd door DICTU (EZK). De ministeries moeten bij gebruik met hen een overeenkomst af te sluiten.

- https://www.avgregisterrijksoverheid.nl/Ministerie_van_Algemene_Zaken/index.html
- https://www.avgregisterrijksoverheid.nl/Ministerie_van_Binnenlandse_Zaken_en_Koninkrijksrelaties/index.html
- https://www.avgregisterrijksoverheid.nl/Ministerie_van_Buitenlandse_Zaken/index.html
- Ministerie van Defensie. https://puc.overheid.nl/mp-bundels/doc/PUC_237438_10/20180525/ ; https://zoek.officielebekendmakingen.nl/stcrt-2018-28293.html; https://wetten.overheid.nl/BWBR0040915/2018-05-25; https://www.defensie.nl/onderwerpen/privacyrechten/privacyrechten-bij-defensie
- https://www.avgregisterrijksoverheid.nl/Ministerie_van_EZK_en_Ministerie_van_LNV/index.html
- https://www.avgregisterrijksoverheid.nl/Ministerie_van_Financien/index.html
- https://www.avgregisterrijksoverheid.nl/Ministerie_van_Infrastructuur_en_Waterstaat/index.html
- https://www.avgregisterrijksoverheid.nl/Ministerie_van_Justitie_en_Veiligheid/index.html
- https://www.avgregisterrijksoverheid.nl/Ministerie_van_Onderwijs_Cultuur_en_Wetenschap/index.html
- https://www.avgregisterrijksoverheid.nl/Ministerie_van_Sociale_Zaken_en_Werkgelegenheid_/index.html
- https://www.avgregisterrijksoverheid.nl/Ministerie_van_Volksgezondheid_Welzijn_en_Sport_/index.html
- https://www.digitaleoverheid.nl/nieuws/best-practice-centrale-verwerkingsregistratie-avg/

Wie moeten een register van verwerkingen bijhouden?

Nagenoeg elke organisatie moet een register van verwerkingen bijhouden. In plaats van verwerkingen aan te melden bij de Autoriteit Persoonsgegevens, moeten organisaties nu de verwerkingen bijhouden in een eigen register.

Wanneer geldt de registratieplicht?

- Voor ondernemingen of organisaties met meer dan 250 personen in dienst
- Wanneer verwerkingen worden gedaan met een hoog risico
- Wanneer niet-incidentele verwerkingen worden gedaan
- Wanneer er verwerkingen van bijzondere categorieën persoonsgegevens of strafrechtelijke gegevens worden gedaan

Wat staat er in het register?

In het register staan allereerst de contactgegevens van de eigenaar van het register en - wanneer van toepassing - van de Functionaris Gegevensbescherming van de organisatie. Op deze manier weten betrokkenen met wie zij contact kunnen opnemen met vragen over hun gegevens. Daarnaast wordt er opgenomen welke verschillende verwerkingen er worden gedaan, de verwerkingsdoelen per verwerking, een beschrijving van de categorieën van betrokkenen en welke persoonsgegevens er van deze mensen worden verwerkt. Bovendien wordt er vastgelegd of er persoonsgegevens worden doorgegeven naar derde partijen, wie deze partijen zijn en of er ook doorgifte naar derde landen gebeurt. Ook wordt er indien mogelijk in het register vastgelegd welke gegevens voor hoe lang bewaard worden. Tot slot wordt er in het algemeen beschreven welke technische en organisatorische maatregelen zijn getroffen om de persoonsgegevens te beveiligen.

Welke concrete aanbevelingen voor het verwerkingsregister door de AP?

1. Benoem hoe lang en met welk doel je persoonsgegevens wil bewaren. Onder de Europese privacywetgeving is het niet toegestaan persoonsgegevens langer te bewaren dan noodzakelijk is voor het doel waarmee ze verzameld zijn. Ook moeten organisaties kunnen motiveren waarom ze deze gegevens verzamelen.
2. Neem de contactgegevens van de verwerkingsverantwoordelijke op in het register.
3. Zorg voor een overzichtelijk bestand van alle verwerkingen van persoonsgegevens waarin gebruikers eenvoudig kunnen navigeren.
4. Geef duidelijk aan op welke locatie of in welk bestand persoonsgegevens bewaard worden en neem deze locaties of bestanden op in het register. Deze informatie is relevant als mensen een verzoek om inzage of verwijdering indienen.
5. Maak duidelijk welk doel bij welke verwerking hoort. Alleen een opsomming van de verwerkingen per afdeling in combinatie met een opsomming van de diverse doeleinden van de verwerkingen is niet voldoende.

60. MAAS. Register van datalekken

Wat zegt de Autoriteit Persoonsgegevens over datalek?

- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken
- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/voorbereiding-op-de-avg#stap-7-meldplicht-datalekken-5897
- https://autoriteitpersoonsgegevens.nl/nl/nieuws/datalek-door-ransomware-wat-moet-u-doen

Haastige spoed is wel zo goed?
Is er sprake van een datalek, of ontvang je signalen dat daarvan sprake kan zijn? Vraag door en doe vooral onderzoek, maar wacht niet te lang met melden. Neem het zekere voor het onzekere en doe, als het niet anders kan, een voorlopige melding. Schakel je een derde in om gegevens voor je te verwerken? Spreek dan heel duidelijk af dat ieder datalek altijd direct wordt gemeld, ook al is het datalek al opgelost en zijn de gevolgen onduidelijk of gering. Hoe die afspraken eruit zouden moeten zien? In veel meer gevallen dan vaak gedacht zijn beide partijen verantwoordelijk.

Wanneer is er sprake van een datalek?
Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident moet u bijvoorbeeld denken aan het kwijtraken van een USB-stick, de diefstal van een laptop of aan een inbraak door een hacker. Er is dus sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als de verwerker onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kan uitsluiten.

Heeft MAAS een datalek protocol?
Ja:

- Hoofdproces in het Blue Book
- Incidentresponse protocol zodat duidelijk is welke stappen doorlopen moeten worden op het moment dat een incident wordt geconstateerd.

Meldt MAAS alle beveiligingslekken?
Nee, als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. Er hoeft dan geen melding te worden gedaan aan de Autoriteit Persoonsgegevens.

Registreert MAAS alle datalekken?
Ja, je moet alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan.

Wat zijn de plichten bij een datalek?
Het datalek moet je bij de Autoriteit Persoonsgegevens melden als dit leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Of als een aanzienlijke kans bestaat dat dit gebeurt. Organisaties moeten de betrokkenen in sommige gevallen ook informeren over het datalek. Dit moet als het datalek waarschijnlijk ongunstige gevolgen heeft voor hun persoonlijke levenssfeer.

Welke drempel voor melden aan de toezichthouder?
Een datalek dient te worden gemeld bij de AP als er, kort gezegd, sprake is vaneen doorbreking van de beveiliging die (een aanzienlijke kans op) ernstige nadelige gevolgen heeft. Deze hoge drempel is geïmplementeerd om nodeloze melding en te voorkomen. Daarnaast iedere inbreuk in verband met persoonsgegevens tenzij niet waarschijnlijk is dat deze een risico inhoudt. Denk aan 'gevoelige gegevens' o.a. bijzondere persoonsgegevens, financiële gegevens, wachtwoord/inlognaam combinatie. Als er geen sprake is van het lekken van bijzondere persoonsgegevens dan moet op grond van de 'aard' en 'omvang' van de gelekte gegevens worden bepaald of een melding vereist is.

Welke drempel voor melden aan de betrokkene?
Een melding aan de AP moet plaatsvinden bij elk incident met betrekking tot persoonsgegevens tenzij niet waarschijnlijk is dat het datalek een risico inhoudt. Een melding aan de betrokkene dient vervolgens plaats te vinden indien het datalek waarschijnlijk een hoog risico inhoudt. Hier ligt de drempel voor melden aan de betrokkene hoger dan voor het melden aan de AP. Voor organisaties betekent dit dat na melding aan de AP een daadwerkelijke nieuwe afweging gemaakt moet worden voor melding aan de betrokkene. Ten aanzien van het informeren van de betrokkene vermeldt de AVG drie uitzonderingen:

- Als er sprake is van goede encryptie, hoeft de betrokkene niet te worden geïnformeerd.
- Informeren niet vereist als dit onevenredig veel inspanning kost.
- Indien de verwerkingsverantwoordelijke achteraf maatregelen heeft genomen om te zorgen dat het hoge risico zich waarschijnlijk niet meer voor zal doen, is melding aan de betrokkene niet vereist. Er wordt een voorbeeld gegeven van een hacker die data heeft gestolen waarbij de hacker kan worden opgepakt voordat hij de data heeft verspreid. In een dergelijk geval heeft het datalek al plaatsgevonden maar zijn er dusdanige maatregelen genomen dat er geen risico op verdere verspreiding is. Als de hacker niets met de gegevens heeft kunnen doen, is er geen sprake van een hoog risico voor betrokkenen zodat de melding ook al op basis daarvan niet vereist zou zijn.

Wat is de termijn voor melding van een datalek?
Een melding aan de toezichthouder moet in beginsel binnen 72 uur plaatsvinden. Van belang is om te bepalen wanneer deze termijn gaat lopen. De 72 uur termijn gaat lopen op het moment dat de verwerkingsverantwoordelijke kennis heeft genomen van ("aware is") een datalek dat gemeld moet worden. Er moet volgens de Guidelines sprake zijn van een 'reasonable degree of certainty' dat het datalek gemeld moet worden. Om tot deze mate van zekerheid te komen, heeft de verantwoordelijke een 'short period of investigation' om te bepalen of het incident gemeld moet worden. Dit betekent dat het starten van de termijn niet afhankelijk is van een ontdekking door de bewerker en dat de verwerkingsverantwoordelijke in bepaalde gevallen tijd heeft om te bepalen of er sprake is van een datalek voordat de termijn start. Dit geeft de verwerkingsverantwoordelijke meer tijd maar zorgt er tevens voor dat de termijn niet meer op een vast moment start. Organisaties moeten bepalen wanneer ze geacht worden 'aware' te zijn. De Guidelines geven verder aan dat de verwerker een verlengstuk is van de verwerkingsverantwoordelijke. Dit betekent dat het moment waarop de verwerker 'aware' wordt, de verwerkingsverantwoordelijk ook geacht wordt 'aware' te zijn. De 72 uur gaat in dat geval al lopen vanaf ontdekking door de verwerker. Bij ontdekking van een incident door de verwerker (hetgeen vaak het geval zal zijn) moet eerst bepaald worden of de verwerker 'aware' was. Zo ja, dan is de verwerkingsverantwoordelijke dat ook en begint de 72 uur termijn op dat moment. Zo nee, dan moet worden bepaald of de verwerkingsverantwoordelijke 'aware' is op het moment dat hij de melding ontvangt. Als dat zo is, heeft hij 72 uur om te melden. Zo niet, dan heeft hij een beperkte tijd om het incident te onderzoeken. Als hij ergens gedurende dit onderzoek 'aware' wordt, start de 72 uur termijn op dat moment.

Vastlegging argumentatie
Als verantwoordelijke zorg je ervoor dat je in verwerkersovereenkomsten met je verwerkers vastlegt dat zij tijdig datalekken die ze signaleren bij jou melden (binnen 24 uur), zodat jij kunt voldoen aan de termijn van 72 uur.
Als verantwoordelijke houd je een register van alle 'inbreuken in verband met persoonsgegevens' bij zodat je altijd kunt aantonen waarom je wel of niet tot melding bent overgegaan. Zorg voor gedegen vastlegging van je argumentatie. Advies is om hetzelfde te doen als verwerker zijnde;
Wanneer je moet melden aan betrokkene, maar deze niet te pakken kunt krijgen, doe je een openbare mededeling. Denk aan gedateerde gegevens waardoor een persoon niet meer te bereiken is.

Is bulkmail naar 'aan' of 'cc' een datalek?
Ja, bij bulkmail kennen de ontvangers elkaar niet. Wanneer de e-mailadressen zichtbaar zijn voor alle ontvangers kan er daarom sprake van een datalek, gebruik daarom de bcc-optie.

Is gegevens onbeveiligd delen via WeTransfer (of vergelijkbaar) een datalek?
Wanneer een bestand via internet gedeeld wordt op basis van een link, is deze link in principe te raden door vreemden of opnieuw te delen met onbevoegden. Zorg ervoor dat bestanden altijd beveiligd zijn met een wachtwoord wanneer geen alternatief beschikbaar is om het bestand te delen. Of maak gebruik van het veilige alternatief, waarmee je makkelijk en veilig grote bestanden kunt delen (encrypted).

Als een printje blijft liggen bij kopieermachine / printer een datalek?
Mogelijk, een lijst met persoonsgegevens blijft liggen bij een printer. Zelfs als deze lijst blijft liggen kan niet gegarandeerd worden dat er geen foto of kopie van is gemaakt. Zorg daarom dat je altijd bij de printer staat als die je documenten print en neem je printjes meteen mee naar je werkplek.

61. MAAS. Verwerkersovereenkomst

Wat zegt de Autoriteit Persoonsgegevens over de Verwerkersovereenkomst c.q. verwerkingsovereenkomst?

- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verwerkers#wanneer-moet-ik-een-verwerkersovereenkomst-afsluiten-7101

Wat zeggen anderen:

- https://www.privacy-friendly.nl/opinie/14
- https://www.ploum.nl/persoonsgegevens-verwerker-of-verantwoordelijke/

Wat is een verwerkersovereenkomst?
In een verwerkersovereenkomst wordt vastgelegd over welke data MAAS mag beschikken. Ook staat daarin hoe lang, wanneer en onder welke voorwaarden die data verwerkt mag worden.
De verantwoordelijkheid voor het afsluiten van de overeenkomst ligt altijd bij de partij die de data verstrekt; de verantwoordelijke. MAAS beschikt over een verwerkersovereenkomst die voldoet aan de regelgeving in de AVG. Deze kan op aanvraag worden opgesteld.

Moet verwerkersovereenkomsten afsluiten met je bank, verzekeraar en zelfs met de Belastingdienst?
Deze derde partijen ontvangen persoonsgegevens van MAAS. Dit is nodig voor de uitvoering van de diensten die zij leveren. Om te weten of je met hen een verwerkersovereenkomst moet afsluiten moet vastgesteld worden of zij onder de AVG de rol van ‘verwerker’ hebben. Met een organisatie die zelf verantwoordelijke is hoeft namelijk geen verwerkersovereenkomst te worden afgesloten. Je bent verantwoordelijke wanneer je het doel en de middelen van de verwerking bepaalt. Wanneer MAAS persoonsgegevens van medewerkers deelt met een verzekeraar dan verwerkt deze verzekeraar de persoonsgegevens voor eigen doeleinden. Zij bepalen in grote mate zelf het doel en de middelen van de verwerking. Zo bepaalt een verzekeraar bijvoorbeeld zelf hoe zij de data beveiligen, met welke verwerkers ze samenwerken, en informeren zij zelf de betrokkene over de verwerking in een privacy statement. In het geval van een datalek zullen zij dit zelf melden aan de toezichthouder, en indien nodig aan de betrokkene. Doordat zij die invloed hebben op de verwerkingen zijn ze verantwoordelijke. Ze verwerken niet op instructies van iemand. Ook wanneer de samenwerking met jullie eindigt zullen zij de gegevensverwerking niet stoppen, omdat ze de gegevens vanwege wettelijke verplichtingen nog moeten bewaren. Om die reden hoeft een organisatie geen verwerkersovereenkomst af te sluiten. Er is dan geen sprake van een verwerker-verantwoordelijke relatie tussen de organisaties en de verzekeraar. Ze zijn beiden verantwoordelijke voor hun eigen deel van de verwerking. Dit is lastige materie, ook voor juristen is het soms moeilijk om hier een standpunt over in te nemen. Het is belangrijk om de rolverdeling te bekijken per verwerking en niet per partij. Je kunt in een samenwerking namelijk verschillende rollen hebben afhankelijk van de verwerking die je voor elkaar doet.

Wat is MAAS beleid ten aanzien van verwerkingsovereenkomsten?

1. MAAS (Maas International B.V.) is als verwerkingsverantwoordelijke verantwoordelijk voor de rechtmatige en zorgvuldige omgang met persoonsgegevens (AVG artikel 5). Dit betekent o.a. dat MAAS de verplichtingen uit de AVG moet naleven en dat MAAS een dergelijke goede naleving moet kunnen aantonen.
2. Om bovenstaande reden dient bijgevoegde MAAS verwerkersovereenkomst met verwerkers te worden aangegaan en niet een verwerkersovereenkomst opgesteld door de verwerker.

Het is bovendien zeer arbeidsintensief om alle verwerkersovereenkomsten opgesteld door verwerkers te controleren en eventueel aan te passen.

3. Het bijgevoegde model geldt voor verwerkers die een overeenkomst hebben met Maas International B.V.
4. Indien verwerkers een overeenkomst hebben met een andere Maas-vennootschap dan Maas International B.V. dan moet dat worden aangeven. MAAS Legal Counsel past de verwerkersovereenkomst dienovereenkomstig aan.
5. Vanuit MAAS ondertekenen conform Handtekeningenschema MAAS, dus de twee bestuurders of één bestuurder en één gevolmachtigde
6. Als de verwerkersovereenkomst door alle partijen is ondertekend dienen Legal Counsel en de Functionaris Gegevensbescherming een kopie te ontvangen.
   - Legal Counsel bewaart de overeenkomst in een digitaal dossier van MAAS onder N:\Maas\Legal.
   - Functionaris Gegevensbescherming bewaart de overeenkomst in een digitaal dossier van MAAS onder N:\Maas\AVG_GDPR

Is een verwerkersovereenkomst nodig als klanten de persoonsgegevens ten behoeve van een toegangspas opvragen?
Nee. De klant gaat in dit geval geen persoonsgegevens voor MAAS International B.V. verwerken, maar wel persoonsgegevens van MAAS medewerker(s) voor eigen doeleinden verwerken. De klant is dus zelfstandig Verwerkingsverantwoordelijke in het kader van de AVG. Geen verwerkersovereenkomst noodzakelijk.
Verstrekte persoonsgegevens van (een) MAAS medewerker(s) vallen dus onder het klant beveiliggingsbeleid. De klant documenteert alle datalekken en meldt deze aan de Autoriteit Persoonsgegevens. Eventuele aanvullende vragen kan MAAS medewerker direct stellen aan de FG van de klant.

Wanneer is nou een verwerkersovereenkomst nodig?
Het is een misverstand dat als er persoonsgegevens worden verwerkt die van een andere organisatie komen er altijd sprake is van een verwerkersrelatie, en dus een verwerkersovereenkomst nodig is. Dat is helemaal niet zo. Het loont de moeite om goed te kijken naar die onderlinge relatie. Er zijn namelijk drie opties:

1. De ene partij is verwerkingsverantwoordelijke, de ander is verwerker. In het geval van optie 1 moet er een verwerkersovereenkomst gesloten worden.
2. De partijen zijn gezamenlijke verwerkingsverantwoordelijken. Optie 2 brengt met zich mee dat partijen afspraken moeten maken over hoe ze hun gezamenlijke verantwoordelijkheid inrichten.
3. De partijen zijn ieder voor zich verwerkingsverantwoordelijke voor de door hen uitgevoerde verwerkingen. In geval van optie 3 zijn geen nadere privacy rechtelijke afspraken nodig. Ieder moet voor zich de AVG naleven.

Optie 3 doet zich vaker voor dan je zou denken op grond van de storm aan verwerkersovereenkomsten die rond waait. Om te bepalen wie de verwerkingsverantwoordelijke is gaat het erom wie het doel en de middelen voor de verwerking vaststelt. Stelt iemand geen doelen en middelen voor de verwerkingen vast, en verwerkt hij dus alleen persoonsgegevens in opdracht van een ander, dan, en alleen dan, is hij verwerker. Bij het bepalen van wie het doel en de middelen voor de verwerking bepaalt gaat het erom wie de feitelijke invloed heeft op de verwerking van de persoonsgegevens, met andere woorden ‘wie daadwerkelijk de beslissingen neemt en feitelijk bepaalt wat er met de gegevens gebeurt’ (Ministerie van Justitie en Veiligheid, Handleiding Algemene verordening gegevensbescherming, januari 2018, p.32).

Het loont de moeite om telkens goed te analyseren wie feitelijk de beslissingen neemt over de persoonsgegevens. Je komt dan al snel op gezamenlijke verantwoordelijkheid (veel simpeler te regelen dan een verwerkersovereenkomst) of op optie 3: ieder is zelf verantwoordelijk. Dan is er geen nadere overeenkomst nodig.

Wiens verantwoordelijkheid is het sluiten van de verwerkersovereenkomst?
Het woord zegt het al: het sluiten van de verwerkersovereenkomst is natuurlijk in eerste instantie de verantwoordelijkheid van de verwerkingsverantwoordelijke. Maar ook de verwerker heeft belang bij het sluiten van een verwerkersovereenkomst. Indien hij namelijk in strijd met de AVG zelf het doel en de middelen van de verwerking van de persoonsgegevens bepaalt, wordt hij door de AVG zelf als verwerkingsverantwoordelijke beschouwd.

Is telkens juridische toetsing van een verwerkersovereenkomst steeds opnieuw nodig?
De inhoud van de verwerkersovereenkomst wordt in vergaande mate bepaald door de verplichtingen in de AVG. Voor zover de verwerkersovereenkomst niet meer regelt dan door de AVG verplicht is gesteld, is het sluiten van verwerkersovereenkomsten niet ingewikkeld. Maar indien en voor zover in de verwerkersovereenkomsten rechten c.q. verplichtingen worden geregeld die niet (of niet in die mate of op die wijze) door de AVG verplicht zijn gesteld, kunnen tegenstrijdige belangen er voor zorgen dat "botsende" verwerkersovereenkomsten ontstaan.
Het is daarom van belang om verwerkersovereenkomsten juridisch te toetsen alvorens deze te ondertekenen. Indien u in staat bent om bij het sluiten van een verwerkersovereenkomst het MAAS model te gebruiken, is die toetsing overbodig.

Is MAAS de verzendende partij van persoonsgegevens?
Denk dan vooraf na over de hoedanigheid van de ontvangende partij en neem de maatregelen die daarbij horen:

Uitwisseling met een verantwoordelijke	Uitwisseling met een verwerker
grondslag checken; doelbinding checken; juistheid/relevantie gegevens checken; transparantie naleven (afspreken of de verzender of ontvanger transparant is); bij internationale situaties buiten EER: check exportverbod	kwaliteit bewerker checken; bewerkersovereenkomst sluiten; toezien op bewerker; bij internationale situaties buiten EER: check exportverbod.

Mocht er bij de ontvangende verantwoordelijke een datalek optreden, dan is die partij verantwoordelijk voor dat datalek. De verstrekkende verantwoordelijke zou alleen aangesproken kunnen worden op de verstrekking van persoonsgegevens als zodanig. Als die uitwisseling van persoonsgegevens niet rechtmatig was, dan kunnen daar boetes of claims uit voortvloeien. Dat wordt echter niet opgelost door het sluiten van een bewerkersovereenkomst. Dat wordt opgelost door ervoor te zorgen dat de uitwisseling zelf rechtmatig is (of achterwege gelaten wordt).

Is MAAS de ontvangende partij van persoonsgegevens?
Toets dan voordat je verder iets met de gegevens doet of de juiste maatregelen zijn genomen:

Uitwisseling met een verantwoordelijke	Uitwisseling met een verwerker
grondslag checken; doelbinding checken; juistheid/relevantie gegevens checken; transparantie naleven (afspreken of de verzender of ontvanger transparant is); bij internationale situaties buiten EER: check exportverbod	kwaliteit bewerker checken; bewerkersovereenkomst sluiten; toezien op bewerker; bij internationale situaties buiten EER: check exportverbod.

Mocht er bij de ontvangende verantwoordelijke een datalek optreden, dan is die partij verantwoordelijk voor dat datalek.

Ben ik de verwerkingsverantwoordelijke, of ben ik een verwerker?
De verwerkingsverantwoordelijke is degene die 'doel en middelen' bepaalt voor de verwerking. Met andere woorden, de verwerkingsverantwoordelijke bepaalt hoe en waarom er persoonsgegevens worden verwerkt. De verwerkingsverantwoordelijke is de (rechts)persoon die letterlijk de verantwoordelijkheid heeft voor het naleven van de Verordening. De verwerker handelt in opdracht van de verwerkingsverantwoordelijke bij het verwerken van persoonsgegevens, zonder onder diens rechtstreeks gezag te staan. Op de verwerker rust de plicht om de instructies van de verwerkingsverantwoordelijke op te volgen. Daarnaast zijn er enkele bepalingen uit de Verordening ook direct van toepassing op de verwerker. Het afsluiten van een verwerkersovereenkomst is een verplichting voor zowel de verwerkingsverantwoordelijke en de verwerker.
Let er bij dit alles op dat één partij beide hoedanigheden (verantwoordelijke en bewerker) tegelijkertijd kan hebben (voor verschillende onderdelen van het verwerkingsproces).

Is voor on-premise software altijd een verwerkersovereenkomst vereist?
Wordt on-premise software gebruikt waarmee persoonsgegevens zullen worden verwerkt, dan is hierbij niet direct een verwerkersovereenkomst vereist, tenzij de software extern wordt beheerd en niet binnen een eigen ICT-omgeving.

Heeft MAAS een verwerkersovereenkomst met de leasemaatschappij voor bedrijfswagens?
Nee, een leasemaatschappij is zelf de verantwoordelijke waar het gaat om verwerkingen van persoonsgegevens van de MAAS berijders. De leasemaatschappij levert de met MAAS afgesproken mobiliteit, en bepaalt zelf welke doelen en middelen zij daarvoor inzet.

Heeft MAAS een verwerkersovereenkomst bij advies werknemersvoorzieningen en –regelingen (pensioen, arbeidsongeschiktheid, verzuim) nodig?
Maas hoeft geen verwerkersovereenkomst te sluiten wanneer Maas een financieel adviseur inschakelt voor het treffen van regelingen ten aanzien van werknemers (i.v.m. pensioen, arbeidsongeschiktheid, verzuim). Het verwerken van de gegevens van de werknemers geen primaire opdracht is ten behoeve van de werkgever, maar logischerwijs voortvloeit uit van een vorm van dienstverlening die de derde partij aanbiedt. Deze situatie doet zich voor bij de dienstverlening van een financieel adviseur aan de werkgever bij het adviseren en bemiddelen bij regelingen voor werknemers.

Moet MAAS een verwerkersovereenkomst met een pensioenfonds sluiten?
Bedrijfstakpensioenfondsen hebben een eigen doel voor het verwerken van persoonsgegevens van deelnemers. Dit doel is namelijk uitvoering geven aan de verplichtingen die opgenomen zijn in de Pensioenwet. Het doel is niet afkomstig van MAAS als werkgever. Om deze reden zijn pensioenfondsen geen verwerker in de zin van de AVG, maar verwerkingsverantwoordelijke. Een verwerkersovereenkomst tussen een werkgever en een bedrijfstakpensioenfonds is dan ook niet noodzakelijk.

Is een verwerkersovereenkomst met de arbodienst verplicht?
Werkgevers zijn verplicht zich bij te laten staan door een arbodienst/bedrijfsarts in bepaalde situaties. In de Arbeidsomstandighedenwet (Arbowet) staan de situaties waarin de werkgever zich verplicht dient te laten bijstaan door een arbodienst/bedrijfsarts. Hierbij kan gedacht worden aan: het adviseren bij de begeleiding van zieke werknemers en het uitvoeren van het arbeidsgezondheidskundig onderzoek. De arbodienst/bedrijfsarts heeft hiervoor dus een eigen wettelijke verplichting en voert deze taken dan ook uit onder de eigen verantwoordelijkheid. Omdat de arbodienst/bedrijfsarts hiervoor zelf verantwoordelijk is met een eigen wettelijke grondslag, is géén sprake van een verwerker in de zin van de AVG. De arbodienst/bedrijfsarts is in deze situatie de verwerkingsverantwoordelijke.
Er kan geen eenduidig antwoord worden gegeven op de vraag of een verwerkersovereenkomst nodig is met de arbodienst/bedrijfsarts. Dit hangt af van de vraag of de arbodienst enkel en alleen de eigen wettelijke taken uitvoert (geen verwerkersovereenkomst noodzakelijk) of ook in opdracht van de werkgever andere taken uitvoert (wel een verwerkersovereenkomst noodzakelijk). Een van deze taken is bijvoorbeeld het opstellen van een plan van aanpak samen met de zieke werknemer of het uitvoeren van de eerstejaarsevaluatie. Wanneer de arbodienst/bedrijfsarts meer dan slechts advies geeft over voornoemde verplichtingen van de werkgever, dan is de arbodienst/bedrijfsarts verwerker in de zin van de AVG. Ook wanneer de arbodienst/bedrijfsarts in opdracht van de werkgever meer gegevens verwerkt in het systeem, zal een verwerkersovereenkomst nodig zijn.
Een verwerkersovereenkomst met een bedrijfsarts die in dienst is van de werkgever in geen geval noodzakelijk is, omdat er dan sprake is van een gezagsverhouding.

Hoe moet ik de afspraak met een verwerker maken?
De AVG bepaalt dat u, indien u gebruik maakt van verwerkers, de verwerking door die verwerker moet regelen in een overeenkomst of anderszins bindende rechtshandeling.
De verwerkersovereenkomst dient in schriftelijke vorm, waaronder elektronische vorm, te worden opgesteld.

Wij hebben al een overeenkomst met MAAS. Waar hoort deze verwerkersovereenkomst?
De verwerkersovereenkomst wordt als een bijlage aan de bestaande overeenkomst toegevoegd.

Wie heeft verwerkersovereenkomsten nodig?
In een verwerkersovereenkomst wordt onder meer geregeld waar de verwerker aan moet voldoen en wie waarvoor verantwoordelijk en aansprakelijk is. Voor veel zaken die op een computer met de persoonsgegeven gebeuren, worden diensten van derden gebruikt. Deze derden zullen niets met die persoonsgegevens doen wat jij niet wil (ze zullen er waarschijnlijk niet eens naar kijken), maar ze ‘verwerken’ ze wel door ze voor jou op te slaan op een server. Veel services die meteen ook opslag aanbieden, veel online software bijvoorbeeld, zijn ook verwerkers. Met al die partijen moet een verwerkersovereenkomsten gesloten zijn.
Wie moet ervoor zorgen dat er een verwerkersovereenkomst is?
Zowel de verwerkersverantwoordelijke als de verwerker moeten ervoor zorgen dat die overeenkomst er is. De een heeft daar niet per se een grotere verplichting in dan de ander, al heb je

als verwerkersverantwoordelijke natuurlijk wel een grotere verantwoordelijkheid voor de persoonsgegevens op zich. Hoe meer controle een partij over de afspraken wil hebben en hoe meer een partij de aansprakelijkheid wil verkleinen, hoe beter het is om er zelf een op te (laten) stellen en aan de andere partij aan te bieden.

Hoe ga je als verantwoordelijke een verwerkersovereenkomst aan?
Zoals uit artikel 28 lid 1 AVG blijkt, dient een verwerkingsverantwoordelijke er zeker van te zijn dat de verwerker afdoende garanties biedt zodat de bescherming van de rechten van de betrokkene wordt gewaarborgd. In art. 28 lid 3 AVG staan de eisen opgesomd die aan een verwerkersovereenkomst worden gesteld. Binnen de AVG wordt aan de verwerker een grote verantwoordelijkheid toegekend. Dit uit zich onder meer in art. 28 lid 4 AVG. Wanneer je als verwerker een andere verwerker in dienst neemt (de sub-verwerker) en deze te kort schiet in de nakoming dan blijft de verwerker ten aanzien van de verwerkingsverantwoordelijke volledig aansprakelijk. Op grond van art. 28 AVG dient je binnen de verwerkersovereenkomst tenminste de volgende zaken af te spreken:

- het onderwerp en de duur van de verwerking;
- het doel en de aard van de verwerking;
- het soort persoonsgegevens waarop de verwerkersovereenkomst betrekking heeft;
- de categorieën van verwerking van de betreffende betrokkenen;
- de rechten en verplichtingen van de verwerkingsverantwoordelijke.

In tegenstelling van wat soms wordt gedacht, hoeft de verwerkersovereenkomst geen losse overeenkomst te zijn: integendeel! Bij het sluiten van nieuwe overeenkomsten waarbij persoonsgegevens meespelen is het raadzaam om de verwerkers overeenkomst een integraal onderdeel te maken van de overeenkomst.

ie niet heeft zitten slapen, weet het: je moet aan de bak met je klanten want de AVG is nu van kracht. In de contractenwereld betekent dit vooral dat iedereen verwerkersovereenkomsten met elkaar gaat zitten sluiten. Belangrijk, want het is boetewaardig om er geen te hebben terwijl je wel verwerker bent. Vandaar: vier brandende vragen over de verwerkersovereenkomst.

Ben ik eigenlijk wel verwerker?
https://juridox.nl/blog/privacy/vier-brandende-vragen-over-de-verwerkersovereenkomst
Omdat het laten tekenen van een verwerkersovereenkomst een mooi concreet ding is dat je kunt doen met het oog op compliance, sturen sommige bedrijven gewoon iedere relatie een verwerkersovereenkomst. Dat klopt natuurlijk niet, want je moet wel daadwerkelijk verwerker zijn. Verwerker ben je als je in opdracht werkt en daarbij de ander laat bepalen wat je doet (doelen) en waarmee (middelen). Die terminologie is wat verwarrend, omdat veel ICT-dienstverleners met name zelf bepalen hoe zij de opdrachten uitvoeren, namelijk met hun eigen software. Uiteindelijk gaat het dan om de zeggenschap over de doelen, hoe vrij ben je om zelf te zeggen, dit doe ik en dit niet. Daarvoor zijn er helaas geen harde criteria, maar we hebben een wizard gemaakt waarmee je dit (gratis) kunt nagaan.
Ben je geen verwerker, teken dan zeker geen verwerkersovereenkomst.

Moet ik die verwerkersovereenkomst ook echt tekenen?
Nee, zeker niet. Ook niet als de andere partij zegt dat het een formaliteit is of dat deze nieuwe tekst gewoon moet vanwege de AVG. Dat je iets moet tekenen staat vast, want de AVG eist nu eenmaal specifieke afspraken tussen verwerker en verantwoordelijke. Maar dat is niet hetzelfde als moeten tekenen wat je wederpartij je aanlevert.

Het slimste is je eigen verwerkersovereenkomst gereed te hebben of liefst nu nog op te sturen naar je klanten. Dan ligt jouw document er maar alvast en hoef je niet in te gaan op hun document. Maak er dus snel eentje en zorg dat je je klanten voor bent.

Wat moet er écht in een verwerkersovereenkomst?
Omdat het ding verwerkers-'overeenkomst' heet, hebben juristen de neiging het ook echt als een contract op te gaan zetten. Dus vermelding van partijen, uitleg over de dienstverlening, handtekeningen en ga zo maar door. Leuk en aardig maar dát staat niet in de AVG. En echt handig is het ook niet, want de verwerkersovereenkomst moet aansluiten bij het echte contract. Dus vaak staan er óf herhalingen in óf dingen die anders zijn dan de hoofdovereenkomst. Beiden niet echt handig.
De AVG zegt (artikel 28 lid 3) dat het volgende erin moet staan:

- Onderwerp van de verwerking – wat ga je doen en onder welk contract, en waarom jij daarbij verwerker bent
- Duur van de verwerking – hoe lang, meestal natuurlijk de looptijd van het echte contract
- Aard en doel – omschrijving van het wat en waarom
- Het soort persoonsgegevens – meestal in een bijlage uitgeschreven als lijstje, zoals namen, e-mailadressen of IP-adressen
- Categorieën van betrokkenen – van welke mensen zijn die gegevens afkomstig
- Rechten van de verantwoordelijke – dat gaat dan om het recht te mogen toezien op jouw nakoming van de verwerkersovereenkomst, het controleren van je beveiliging en je instructies mogen geven over hoe ze graag willen dat dingen gaan
- Verplichtingen van de verantwoordelijke – met name dat ze instaan voor een goede grondslag (zoals toestemming) en de rechten van betrokkenen netjes afhandelen

Het oplettende lezertje zal nu opvallen dat in deze lijst het woord 'aansprakelijkheid' ontbreekt. Dat is met opzet, want dat hoeft helemaal niet geregeld te worden in de verwerkersovereenkomst. Je staat dan ook in je recht als je de poot stijf houdt en eist dat artikelen over vrijwaring en aansprakelijkheid eruit gehaald worden. Zeker als je dat al gewoon in je hoofdovereenkomst hebt geregeld.

Moet het echt een apart contract zijn?
Nee, dat hoeft niet. De AVG eist dat een "overeenkomst of andere rechtshandeling" wordt verricht om de afspraken over die bullets vast te leggen, en wel schriftelijk, maar zegt niet dat het een apárt document moet zijn. Iedereen doet dat, maar het is nergens voor nodig en zeker niet verplicht. Het is dus prima als je een artikel in je algemene voorwaarden maakt dat je "Verwerking van persoonsgegevens" noemt en waarin je de bovengenoemde punten opneemt.

62. MAAS. Medewerkerbewustzijn

Wat zegt de Autoriteit Persoonsgegevens over de medewerkerbewustzijn?
https://autoriteitpersoonsgegevens.nl/nl/over-privacy/privacyverhalen

Overige
https://www.fgsupport.nl/bewustwordingsprogramma

Wat is medewerkersbewustzijn?
Kennen medewerkers hun privacyrechten voldoende? Weten ze wat ze moeten doen bij een (vermoeden van een) datalek? Het is aan te raden om medewerkers te betrekken bij de AVG. Zij zijn een belangrijke schakel – vergeet hen niet. Praat met hen over privacy, stimuleer goed gedrag en zorg dat de invoering van de AVG niet slechts een papieren exercitie is. Privacy bewustzijn en een cultuur waarin medewerkers zich vrij voelen om privacy kwesties te bespreken, dragen bij aan een goede bescherming van de persoonsgegevens in uw organisatie.

Onderdelen van het bewustwordingsprogramma zijn bijvoorbeeld:

- Een introductie van de uitgangspunten van de AVG.
- Praktische voorbeelden uit het dagelijkse leven.
- Gegevensbescherming bij sociale media, websites, apps en cloud computing.
- Do's & dont's bij het gebruik van computers en smartphones.
- De mogelijke gevolgen van datalekken en cybercriminaliteit.

63. MAAS. Corona app

Wat zegt de AP over Corona gerelateerde zaken:

- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona

Wat zeggen andere bronnen over Corona app en vragen naar vaccinatie?

- https://www.bdo.nl/nl-nl/perspectieven/gebruik-coronacheck-app-door-werkgevers

Wanneer gebruik je de CoronaCheck-app?
Met ingang van 25 september 2021 is het gebruik van de CoronaCheck-app op een aantal locaties (waaronder de horeca en evenementen) verplicht. Bezoekers van deze locaties moeten dan een coronatoegangsbewijs kunnen tonen voordat zij naar binnen mogen. Dit bewijs wordt geleverd in de vorm van het scannen van een QR-code die een groen vinkje laat zien wanneer de bezoeker volledig is gevaccineerd, een recente negatieve testuitslag heeft of is hersteld van een coronabesmetting.

In hoeverre kan een werkgever de CoronaCheck-app gebruiken op de werkvloer?

- Zorgplicht werkgever. Een werkgever is verplicht om te zorgen voor een gezonde en veilige werkomgeving. Sommige werkgevers zouden graag invulling geven aan deze zorgplicht door de CoronaCheck-app te gebruiken, omdat in dat geval aan de voordeur een controle kan plaatsvinden. Het risico op een besmetting op de werkvloer kan daarmee worden verkleind.
- CoronaCheck-app verplichting. Het gebruik van de CoronaCheck-app is echter niet zonder meer mogelijk. De CoronaCheck-app is namelijk alleen verplicht gesteld voor locaties waar activiteiten met een hoog besmettingsrisico plaatsvinden, zoals horeca- en evenementenlocaties. Voor werkgevers in andere sectoren is er dus geen (directe) juridische grondslag om het gebruik van de CoronaCheck-app te verplichten. Bovendien is het gebruik van de CoronaCheck-app alleen verplicht voor bezoekers van de locaties. Bezoekers hebben namelijk de vrije keuze om locaties wel of niet te bezoeken.

CoronaCheck-app door werkgevers te verplichten?
Nee. Vrije keuze om locaties wel of niet te bezoeken hebben werknemers niet, omdat werknemers op grond van de arbeidsovereenkomst de plicht hebben om arbeid te verrichten en in de meeste gevallen van hun werk afhankelijk zijn om in het levensonderhoud te voorzien. Ook zijn er praktische complicaties, nu werknemers die niet zijn gevaccineerd en niet zijn hersteld van een coronabesmetting uiterlijk 24 uur voor elke werkdag een coronatest zouden moeten ondergaan tot het werk te kunnen worden toegelaten. Daarom heeft de wetgever ervoor gekozen om werknemers expliciet uit te sluiten van de groep die kan worden verplicht tot gebruik van de CoronaCheck-app.

Vragen naar de Vaccinatiestatus toegestaan?
Nee. Naast het bovenstaande geldt dat een werkgever geen medische gegevens van zijn werknemers mag verwerken, zoals bijvoorbeeld de vaccinatiestatus. Ook doen werkgevers er goed aan om terughoudend te zijn met het stellen van vragen over de vaccinatiestatus. Gelet op de afhankelijkheidsrelatie tussen een werknemer en werkgever kan een werknemer zich namelijk onder druk gezet voelen om een dergelijke vraag op een bepaalde manier te beantwoorden.
Hiernaast is het de vraag welk doel een vraag naar de vaccinatiestatus dient. Het antwoord mag immers niet worden verwerkt. Ook spelen er risico's in het kader van gelijke behandeling wanneer een werknemer anders zou worden behandeld afhankelijk van de vaccinatiestatus. Een werknemer zou zich in dat geval op het standpunt kunnen stellen dat er sprake is van verboden onderscheid op basis van medische gesteldheid.

Komt er een wetswijziging?
De minister van Volksgezondheid, Welzijn en Sport heeft aangekondigd dat het kabinet wil verkennen of en hoe de CoronaCheck-app in werksituaties gebruikt zou kunnen worden. Hiervoor is echter een wetswijziging nodig. Tot op heden is niet bekend of deze wetswijziging er gaat komen en of er daarmee nieuwe mogelijkheden komen voor werkgevers. Werkgevers doen er goed aan om terughoudend te zijn met het stellen van vragen naar de vaccinatiestatus en mogen hun werknemers op dit moment niet verplichten om een coronatoegangsbewijs te tonen voordat zij de werkvloer betreden.

64. MAAS. Corona mondkapje

Wat zegt de AP over Corona gerelateerde zaken:

- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona

Wat zeggen andere bronnen over mondkapjesplicht?

- https://ploum.nl/kenniscentrum/nieuws/mondkapjesplicht-op-werk-mag-een-werkgever-het-dragen-van-een-mondkapje-verplichten-voor-werknemers?utm_medium=email
- https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBMNE:2021:51 13-01-2021
- https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBNHO:2021:8121 21-09-2021
- https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBNHO:2021:10055 05-11-2021
- https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBMNE:2021:863 05-03-2021

Mondkapjesplicht op werk: mag een werkgever het dragen van een mondkapje verplichten voor werknemers?

De mondkapjesplicht. Na twee jaar kennen wij dit allemaal wel. Na meerdere versoepelingen is momenteel de mondkapjesplicht weer aan de orde binnen in de publieke locaties. Het kan daardoor voorkomen dat het ook verplicht is om op werk een mondkapje te dragen. De praktijk leert dat het nog wel eens voorkomt dat werknemers – om welke reden dan ook – liever geen mondkapje willen dragen tijdens de werkzaamheden.
De vraag die vaak opspeelt is dan ook: mag de werkgever een werknemer verplichten een mondkapje te dragen tijdens de werkzaamheden? En zo ja, op welke wijze kan dit eventueel worden afgedwongen? In dit artikel leest u hier meer over.

Welke rol speelt instructierecht werkgever?

Uit recente rechtspraak blijkt dat het instructierecht van de werkgever een uitkomst kan bieden. De werknemer staat namelijk onder de zeggenschap van de werkgever en de werknemer heeft zich in beginsel te houden aan de instructies van de werkgever. Dit kan echter anders zijn als het instructierecht een ongeoorloofde inbreuk maakt op een grondrecht van de werknemer. Er moet in dat kader dan worden gekeken of deze instructie een legitiem doel dient en of zij een geschikt middel is om dat doel te bereiken.
De werkgever is ten eerste wettelijk verplicht de individuele belangen van haar werknemers te beschermen door zorg te dragen voor een gezonde en veilige werkomgeving. De werkgever moet, voornamelijk gedurende de coronapandemie, ervoor zorgen hetgeen te doen wat nodig is en wat van hem gevergd kan worden om besmetting van haar werknemers op de werkvloer met het virus te voorkomen. Ten tweede heeft de werkgever hier ook een bedrijfsbelang om te beschermen: werkgevers hebben immers een loondoorbetalingsverplichting bij ziekte.
Hoewel de effectiviteit van het mondkapje wordt betwist, is het een maatschappelijk aanvaard middel om verspreiding van het virus te voorkomen. Ook is de inbreuk evenredig in verhouding tot het belang van de werkgever om de hiervoor beschreven doelen te bereiken. Om die reden kan de instructie van het dragen van een mondkapje dan ook worden gegeven door de werkgever, ook al betoogt de werknemer dat de verplichting om een mondkapje te dragen een inbreuk vormt op zijn grondrecht. Er is namelijk een legitiem doel en het mondkapje is tevens een geschikt middel om dat doel te bereiken, en daarom kunnen werknemers gehouden worden zo'n instructie op te volgen.

Differentiatie tussen functies?

Een vraag die vaker voorkomt in de praktijk is of de mondkapjesplicht moet differentiëren naar verschillende functies. In een bedrijf zijn er namelijk medewerkers die veel in contact komen met derden of collega's, maar je hebt ook medewerkers die vrijwel geen contact hebben met anderen tijdens de werkzaamheden. De rechter heeft in een uitspraak van 13 januari 2021 geoordeeld dat de werkgever er belang bij heeft om ten aanzien van de instructie over het dragen van een mondkapje één lijn te trekken binnen het bedrijf. Het dragen van een mondkapje kan alleen maar effectief zijn als iedereen zich gezamenlijk aan houdt. Werkgevers moeten zorgen voor een veilige en gezonde werkomgeving en dat is alleen mogelijk met een eenduidig beleid.

Loonbetaling opschorten en ontzegging van het werk?
Uit rechtspraak blijkt dat werkgevers de loonbetaling van werknemers mogen opschorten en de toegang tot het werk mogen ontzeggen als de instructies niet worden opgevolgd en het niet duidelijk is dat werknemer onvoorwaardelijk bereid is de instructie alsnog op te volgen. Zodra de werknemer wél weer onvoorwaardelijk bereid is de instructie op te volgen, vervalt daarmee de grondslag aan de opschorting van het loon en aan de non-actiefstelling.

Ontbinding arbeidsovereenkomst op de loer?
Het weigeren van de werknemer om de instructie van het dragen van een mondkapje op te volgen, kan soms leiden tot een verstoorde arbeidsverhouding. Dit blijkt uit een recente uitspraak van de rechtbank Noord-Holland van 21 september 2021 waarin de rechter oordeelde dat de werknemer verplicht is die instructie op te volgen. De werknemer in het geding bleef zich verzetten tegen de instructie om een mondkapje te dragen. Hierover zijn conflicten ontstaan, welke meermaals zijn geëscaleerd. Hierdoor oordeelde de rechter dat de arbeidsverhouding duurzaam en onherstelbaar verstoord is.
Het weigeren een mondkapje te dragen zou zelfs kunnen leiden tot een ontbinding op grond van (ernstig) verwijtbaar handelen van de werknemer. Dit blijkt uit een uitspraak van de rechtbank Noord-Holland van 5 november 2021 waarin de werknemer bij herhaling heeft geweigerd een mondkapje te dragen tijdens de werkzaamheden, met als gevolg dat hij zijn werkzaamheden niet kon uitvoeren. De werkgever heeft de werknemer hier meerdere malen op aangesproken en de werknemer tevens gewaarschuwd voor de gevolgen voor zijn dienstverband. Omdat door het weigeren een mondkapje te dragen, de werknemer de voortgang van het werkproces belemmert, met als risico dat klanten van werkgever hun opdrachten intrekken, oordeelde rechter dat de werknemer (ernstig) verwijtbaar heeft gehandeld. Hierdoor verloor de werknemer tevens het recht op een transitievergoeding.

Risico toekenning billijke vergoeding?
In een uitspraak van rechtbank Midden-Nederland van 5 maart 2021 kende de rechter een billijke vergoeding toe aan de werknemer. Dit gebeurt in gevallen waarin de ontbinding van de arbeidsovereenkomst het gevolg is van ernstig verwijtbaar handelen of nalaten van de werkgever. Hier was dat het geval, omdat er sprake was van een verstoorde verhouding maar de werkgever niet haar verantwoordelijkheid had genomen om tot herstel van de onderlinge verhoudingen te komen. Er is geen één keer geprobeerd het gesprek aan te gaan met werknemer om zijn kant van het verhaal te horen. Omdat de werkgever op deze manier heeft gezorgd voor een verdere escalatie in plaats te zoeken naar een oplossing, oordeelde de rechter dat de werkgever ernstig verwijtbaar heeft gehandeld als gevolg waarvan aan de werknemer een billijke vergoeding werd toegekend.

Concluderend
De verplichting om een mondkapje te dragen op het werk valt onder het instructierecht van de werkgever en werknemers zijn verplicht deze instructies op te volgen.

Als de instructies niet worden opgevolgd en het niet duidelijk is dat werknemer onvoorwaardelijk bereid is de instructie (alsnog) op te volgen, kan de werkgever de loonbetaling opschorten en de werknemer toegang tot het werk ontzeggen. Dit kan echter niet meer wanneer blijkt dat de werknemer wel weer onvoorwaardelijk bereid is de instructie op te volgen.

De arbeidsovereenkomst kan mogelijk worden ontbonden indien de instructie om een mondkapje te dragen stelselmatig niet wordt opgevolgd. Werkgevers moeten hierbij wel letten op het feit dat ze de kwestie op enige manier eerst met de betreffende werknemer moeten bespreken. Dit is niet alleen raadzaam ten aanzien van het voorkomen van verdere escalatie, maar ook in het kader van het risico tot betaling van een billijke vergoeding ingeval van ontbinding.

65. HR. Arbodienst

Wat zegt de Autoriteit Persoonsgegevens over Arbodienst?

Wat betekent de Europese privacywetgeving voor de dienstverlening van Arbo?
Arbo dienstverleners maken in hun dagelijks werk sinds jaar en dag gebruik van persoonlijke gegevens van werknemers. Zij voldoen daarbij vanzelfsprekend aan de geldende wet- en regelgeving in Nederland.
Zo zijn de volgende wetten voor hun dienstverlening van toepassing:

- de Wet op de Geneeskundige Behandel Overeenkomst, hierin wordt voor Arbo dienstverleners en andere zorgdienstverleners bepaald hoe we omgaan met het medisch dossier en de raadpleging en vernietiging ervan.
- de Arbowet, hierin wordt bepaald wat geldend is voor werkgevers en dienstverleners in de bedrijfsgezondheidszorg als het gaat om de veiligheid en gezondheid van medewerkers.
- de Privacywet, hierin wordt bepaald hoe om moet worden gegaan met de bescherming van persoonsgegevens.

In aanloop naar de Europese privacywetgeving (AVG), die vanaf 25 mei 2018 geïmplementeerd moet zijn, is de werkwijze op een aantal punten uitgebreid. Het gaat om de volgende onderwerpen:

1. Aanpassing van het bestaande Privacyreglement
2. Aanstelling van een Register functionaris gegevensbescherming
3. Hanteren van een verwerkingsregister
4. Data Privacy Impact Assessment
5. Aanpassing van de procedure voor datalekken
6. Uitbreiding van informeren en trainen eigen medewerkers
7. Verwerkersovereenkomsten hanteren inclusief alle toeleveranciers
8. Rechten van de betrokkenen borgen met betrekking tot vastgelegde persoonsgegevens.

Wat mag ik als werkgever/leidinggevende wel en niet vragen aan een zieke werknemer volgens de Autoriteit Persoonsgegevens?
Wanneer een werknemer zich ziek meldt mag u de volgende gegevens over zijn gezondheid vragen en registreren:

- vermoedelijke duur van het verzuim;
- lopende afspraken en werkzaamheden;
- telefoonnummer en (verpleeg)adres;
- of de werknemer onder een van de vangnetbepalingen van de Ziektewet valt (maar niet onder welke vangnetbepaling);
- of de ziekte verband houdt met een arbeidsongeval;
- of er sprake is van een verkeersongeval waarbij een eventueel aansprakelijke derde betrokken is, in verband met het verhalen van loonkosten op deze derde (regresmogelijkheid).

Vragen naar de gezondheidsklachten van de werknemer of deze schriftelijk vastleggen mag echter niet. Deze privacygevoelige informatie mag alleen de bedrijfsarts verzamelen en verwerken. Dat geldt ook voor de vraag naar de mogelijkheden van de werknemer. Komt de zieke werknemer spontaan met deze informatie, dan mag u die ook niet schriftelijk vastleggen. Heeft de bedrijfsarts de mogelijkheden vastgesteld, dan kunt u met de werknemer het vervolgens wel over de beperkingen en mogelijkheden hebben.

Wat doet Arbo Dienstverlener met de persoonlijke gegevens van mijn werknemers?
Arbo Dienstverlener verwerkt de persoonsgegevens van uw werknemer met wie we een behandelrelatie hebben enkel en alleen voor de uitvoering van haar wettelijk taak als arbodienstverlener. Arbo Dienstverlener hanteert een privacyreglement. Hierin staat van wie deze informatie is, hoe wij de gegevens vastleggen en wie deze gegevens mag bekijken en wie niet.

Moeten werknemers vooraf instemmen met het delen van persoonsgegevens met een arbodienst?
Nee, de arbodienst vraagt alleen de strikt noodzakelijke gegevens op voor de uitvoering van haar wettelijke taak. Hiervoor is niet nogmaals extra instemming van de betrokken werknemer nodig. De OR heeft in algemene zin conform de Arbowetgeving instemmingsrecht op de afspraken tussen de werkgever en de arbodienstverlener.

Op basis van welke grondslag mag Arbo Dienstverlener persoonsgegevens verwerken?
Als uitvoerder van de Arbowet verwerkt Arbo Dienstverlener de gegevens op basis van de wettelijke verplichting (de grondslag), Arbo Dienstverlener bepaalt het doel en de middelen van de gegevensverwerking en is daarom verantwoordelijke onder de AVG.

Wat betekent de nieuwe AVG wetgeving voor u als werkgever bij de uitwisseling van informatie met een arbodienst?
Als werkgever bent en blijft u ervoor verantwoordelijk dat de juiste informatie over medewerkers met wie wij een behandelrelatie aangaan, naar Arbo Dienstverlener wordt gestuurd. Door gebruik te maken van een gestandaardiseerde en geautomatiseerde berichtenkoppeling doet u dat op een betrouwbare en veilige manier. Met de gangbare personeelsinformatiesystemen heeft Arbo Dienstverlener een standaard koppeling op basis van de Verzuimstandaard 2017 beschikbaar om rechtmatig informatie uit te kunnen wisselen in het kader van de verzuim- en re-integratiebegeleiding.

Wat betekent de nieuwe wetgeving voor de contracten tussen werkgever en Arbo Dienstverlener?
Het doorvoeren van wijzigingen die voortkomen uit wet- en regelgeving maakt integraal onderdeel uit de dienstverlening. De wijzigingen die voortkomen uit de AVG zijn vastgelegd in het vernieuwde Privacyreglement en dit maakt dan ook onderdeel uit van het geldende contract. Op deze wijze bent u er als werkgever ook van verzekerd dat u voldoet aan de AVG. Een voorbeeld van een vernieuwd privacyreglement is van een arbodienstverlener is beschikbaar via deze link .

Welke informatie mag er in het kader van de bedrijfsgezondheidszorg uitgewisseld worden tussen werkgever en arbodienstverlener?
Voor het uitwisselen van de juiste informatie hanteren we binnen onze branche de verzuimstandaard voor verzuim- en re-integratiebegeleiding. Dit is een set aan gegevens die is gebaseerd op de geldende wet- en regelgeving en dus ook op de AVG. Deze standaard is getoetst door de brancheorganisatie, waardoor u in dit kader ook geen extra privacy assessment (DPIA) hoeft uit te voeren.

Voor het uitvoeren van Preventief Medische Onderzoeken, Risico-inventarisaties en -evaluaties en keuringen vraagt Arbo Dienstverlener uitsluitend informatie van de werkgever en cliënt dan noodzakelijk is voor uitvoering van deze wettelijke taken.

Wanneer heeft een Arbo Dienstverlener de wijzigingen die voortkomen uit de AVG volledig geïmplementeerd?

Arbo Dienstverlener voldoet aantoonbaar aan alle nieuwe werkprocessen die voortkomen uit de AVG met een aantal items:

a. Arbo Dienstverlener beschikt over een aangepast privacyreglement, waarmee we klanten en cliënten informeren over de manier waarop we invulling geven aan de Privacywetgeving. De informatie stellen we via onze website beschikbaar.
b. Arbo Dienstverlener heeft het ISO 27001 en ISO9001 certificaat voor informatiebeveiliging en het certificaat arbodienstverlening. Toetsing van de werkwijze vindt regelmatig plaats door externe auditors. Arbo Dienstverlener werkt continu aan het verbeteren van de bescherming van informatie en blijft hierin investeren. De Corporate Informatie Security en Privacy Officer is geregistreerd als Functonaris Gegevensbescherming en houdt hier onafhankelijk toezicht op.
c. Arbo Dienstverlener registreert alle informatieverwerkingen in een verwerkingenregister, dat zorgvuldig wordt beheerd.
d. Bij wijzigingen in de verwerking van persoonsgegevens is Arbo Dienstverlener verplicht om een formele en gedocumenteerde review te houden van de risico's en de te nemen maatregelen om deze gegevens te beschermen. Dit heet in de AVG een 'Data Privacy Impact Assessment'. Deze procedure is geborgd binnen onze werkprocessen.
e. Medewerkers van Arbo Dienstverlener zijn verplicht om alle datalekken direct, en zonder vertraging te melden bij de Corporate Informatie Security en Privacy Officer. Na beoordeling handelt deze conform de wetgeving.

De Autoriteit Persoonsgegevens houdt voor de overheid toezicht op de naleving van de AVG.

Wat betekent de AVG voor mijn werknemers als het gaat om zijn of haar eigen gegevens en het recht op informatie, inzage, correctie, gegevensuitwisseling en gegevensoverdracht?
Arbo Dienstverlener heeft zich als dienstverlener in de bedrijfsgezondheidszorg te houden aan meerdere wetten, zoals de Wet op de Geneeskundige Behandel Overeenkomst (WGOB), de Arbowetgeving en de Privacywetgeving.

Inzage in het medisch dossier of keuringsrapport en de rechten die een werknemer heeft om dit te raadplegen en te laten vernietigen vallen onder de wetgeving van de WGBO. Dat betekent dat de AVG hier niet op van toepassing is. Een werknemer kan een schriftelijk verzoek tot inzage indienen bij Arbo Dienstverlener. Stuur dit verzoek per mail aan binnendienst@arbodienstverlener.nl. Binnen zes weken na aanvraag, ontvangt de werknemer bericht van ons over de manier waarop de informatie kan worden ingezien.

Moet ik als werkgever een gezamenlijke verwerkersovereenkomst opstellen met Arbo Dienstverlener?
Nee. In het kader van de AVG treedt Arbo Dienstverlener op als verantwoordelijke voor de verwerking van de persoonsgegevens. Dit betekent dat Arbo Dienstverlener geen verwerker is en het opstellen van een verwerkersovereenkomst om die reden niet nodig is.

Moet ik als werkgever een Data Privacy Impact Assessment (DPIA) doen als ik van arbodienst wissel?
Normaal gesproken dient u met een nieuwe dienstverlener een DPIA op te stellen. Wanneer u echter als werkgever al vanuit de verzuimstandaard werkt en bij wisseling van arbodienst op dezelfde manier blijft werken, is het opstellen van een nieuwe DPIA niet nodig.

De scope van DPIA vanuit de werkgever betreft het verzamelen van de noodzakelijke persoonsgegevens en het ter beschikking stellen aan de arbodienst. De verwerking van de persoonsgegevens valt onder verantwoording van de arbodienst.

66. HR. Diversiteit en Inclusie

Wat zegt de Autoriteit Persoonsgegevens over Diversiteit & Inclusie?
Niets…

Wat zeggen andere bronnen over AVG en Diversiteit & Inclusie?

- https://www.considerati.com/nl/kennisbank/diversiteit-inclusie-avg.html
- SER Diversiteit in Bedrijf (onderdeel van de Sociaal Economische Raad) biedt een algemeen
- charterdocument over de verwerking van persoonsgegevens voor diversiteitsbeleid. Dat
- document is te vinden op: https://www.ser.nl/-/media/ser/downloads/thema/diversiteitinbedrijf/publicaties/2021/Charterdocument_meten-is-weten.pdf

Waarom het uitvoeren van een onderzoek naar diversiteit en inclusie binnen organisatie overwegen?
Diversity wins: how inclusion matters" is de titel van een rapport dat McKinsey in 2020 publiceerde. Uit hun analyse blijkt dat "bedrijven in het topkwartiel voor zowel gender als etnische diversiteit 12 procent meer kans hebben om beter te presteren dan alle andere bedrijven in de dataset". Er is dus een goede reden om te investeren in programma's gericht op het bevorderen van diversiteit en inclusie (D&I). Hoewel organisaties dit erkennen, worstelen organisaties met het vinden van betrouwbare methoden om succes te meten en te begrijpen of hun programma's echt werken. In de praktijk houden dergelijke methoden in dat er diversiteitsgegevens van werknemers verzameld moeten worden om inzicht te krijgen in de situatie van vandaag en de toekomst om het effect van diversiteitsprogramma's te kunnen meten. Door de wereldwijd uiteenlopende wet- en regelgeving als het gaat om de verwerking van "bijzondere persoonsgegevens" is de oplossing niet zo eenvoudig; vooral niet voor organisaties die in meerdere landen actief zijn.

Niet een maar twee rechtsgrondslagen?
Op grond van de Algemene verordening gegevensbescherming (AVG) moet elke verwerking van persoonsgegevens gebaseerd worden op een grondslag, die is opgenomen in artikel 6 AVG. Daarnaast worden in de AVG bepaalde soorten persoonsgegevens aangemerkt als "bijzondere persoonsgegevens" die specifieke bescherming behoeven, omdat de aard van deze gegevens met zich meebrengt dat de verwerking ervan aanzienlijke risico's kan opleveren voor de fundamentele rechten en vrijheden van personen. Dit soort gegevensverwerkingen is daarom in beginsel verboden, tenzij er op grond van artikel 9, lid 2, een uitzondering geldt.
In het kader van de uitvoering van D&I-onderzoeken is het waarschijnlijk, zo niet zeker, dat organisaties belang hebben bij het verzamelen en verwerken van bijzondere persoonsgegevens van hun werknemers om de niveaus van diversiteit binnen verschillende categorieën te kunnen bepalen. Dit betekent dat er niet alleen een grondslag op basis van artikel 6 AVG moet worden vastgesteld, maar dat ook moet worden voldaan aan een uitzondering op grond van artikel 9, lid 2, AVG om te waarborgen dat D&I-onderzoeken rechtmatig worden uitgevoerd.

Welke D&I-gegevens gelden als bijzondere persoonsgegevens?
Niet bij alle D&I-onderzoeken worden bijzondere persoonsgegevens verwerkt, maar binnen dergelijke onderzoeken spelen doorgaans enkele of alle van de volgende categorieën een rol:

- Raciale of etnische gegevens
- Politieke meningen
- Religieuze of filosofische overtuigingen
- Seksuele geaardheid of iemands seksleven

- Gezondheidsgerelateerde gegevens, zoals invaliditeit of andere beperkingen

Overigens, worden gender of gegevens betreffende iemands geslacht in beginsel niet als bijzondere persoonsgegevens aangemerkt. Het is echter minder duidelijk hoe genderidentiteit ('gender identity') onder de AVG moet worden geclassificeerd. Hoewel het niet per definitie is aan te merken als een bijzonder persoonsgegeven is, althans niet direct, is het denkbaar dat er indirect wel dergelijke informatie uit kan worden afgeleid (zoals informatie over iemands gezondheid of seksuele geaardheid). Zo oordeelde de gegevensbeschermingsautoriteit in Noorwegen bijvoorbeeld in een zaak tegen Grindr dat het feit dat iemand een Grindr-gebruiker is, is aan te merken als een bijzonder persoonsgegevens, omdat dit er sterk op wijst dat de gebruiker in kwestie tot een seksuele minderheid behoort. Voor meer informatie over wanneer persoonsgegevens als bijzondere persoonsgegevens kunnen worden aangemerkt door middel van een gevolgtrekking, verwijs ik naar mijn eerdere blog daarover.
Al met al, worden organisaties aangemoedigd om zorgvuldig na te gaan of de gegevens die zij voornemens zijn te verzamelen, kunnen worden aangemerkt als bijzondere persoonsgegevens, hetzij vanwege hun inherent gevoelige aard (direct), hetzij bij wijze van gevolgtrekking (indirect). Dat is een voorwaarde om te bepalen welke grondslag nodig kan zijn.

Op welke rechtsgrondslag kunt u zich beroepen?
Dit is waar een wisselend juridisch landschap inzake gegevensbescherming de zaken compliceert. Artikel 9, lid 2, AVG voorziet in uitzonderingen op het verbod om bijzondere persoonsgegevens te verwerken, waaronder (i) toestemming en (ii) wanneer de verwerking noodzakelijk is met het oog op de uitvoering van de verplichtingen en de uitoefening van de specifieke rechten van de verwerkingsverantwoordelijke of de betrokkene op het gebied van het arbeidsrecht en het socialezekerheids- en socialebeschermingsrecht. Deze laatste kan leiden tot aanvullende specifieke uitzonderingen op de AVG die per lidstaat verschillen.
Zo is er in Nederland onder de Uitvoeringswet AVG een vrijstelling die de verwerking van ras en etnische afkomst toestaat als aan bepaalde voorwaarden wordt voldaan. Ter ondersteuning van deze vrijstelling heeft het CBS op verzoek van het ministerie van Sociale Zaken en Werkgelegenheid (SZW) de Barometer Culturele Diversiteit ontwikkeld om dit te meten, mits organisaties meer dan 250 werknemers hebben.
Het bestaan van specifieke vrijstellingen of verplichtingen die de verzameling van D&I-gegevens toestaan of juist vereisen die van land tot land verschillen, leidt tot een situatie waarin er vaak geen one size fits all oplossing is, waardoor wereldwijde D&I-initiatieven op moeilijkheden stuiten. Hierdoor komen organisaties wellicht in de verleiding om de mogelijkheid te onderzoeken om de verwerking op de toestemming van werknemers te baseren. Het probleem hierbij is echter dat toestemming in een dergelijke context zelden wordt beschouwd als vrijwillig gegeven onder de AVG, vanwege het feit dat er sprake is van een onevenwichtige machtsverhouding tussen werkgevers en werknemers.

Wat zou u dan moeten doen?
Hieronder volgen enkele praktische aanbevelingen om in gedachten te houden als u D&I-onderzoeken overweegt:
- Bepaal zorgvuldig het doel van uw D&I-onderzoek.
- Beperk de verzamelde gegevens tot wat nodig is voor deze omschreven doeleinden.
- Probeer, waar mogelijk, de benodigde informatie te verkrijgen via echt anonieme enquêtes.
- Beoordeel of de gegevens die u wilt verzamelen als bijzondere persoonsgegevens kunnen worden aangemerkt.
- Bepaal welke rechtsgrondslag (per jurisdictie) geschikt is voor de categorieën van de verzamelde gegevens.

- Vermijd open invulvelden in enquêtes die bijzondere persoonsgegevens kunnen onthullen die verder gaan dan uw gedefinieerde doeleinden.
- Voer een DPIA uit om ervoor te zorgen dat de privacy beginselen worden nageleefd en dat de rechten van personen adequaat worden beschermd.
- Betrek uw werknemers om hun mening over de beoogde gegevensverzamelingen te vernemen.
- Verzeker uzelf van de steun van de ondernemingsraad als uw organisatie die heeft.
- Zorg ervoor dat D&I-verwerkingsactiviteiten worden geregistreerd in uw verwerkingsregister.

67. HR. Email ex-werknemers

Wat zegt de Autoriteit Persoonsgegevens over de email (ex-)werknemers?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-uitkering/controle-van-personeel

Mag je e-mails bekijken van ex-werknemers?
Waardevolle data zoals de contactgegevens van klanten, het akkoord op een offerte en afspraken hierover zijn doorgaans terug te vinden in de inbox van de werknemer. Maar wat gebeurt er met deze gegevens als de werknemer uit dienst gaat? Mag u e-mail van de ex-werknemer inzien? En hoe lang mag u deze bewaren? En hoe voorkomt u dat belangrijke informatie verloren gaat doordat een – gefrustreerde – werknemer op de delete-knop drukt wanneer hij uw onderneming verlaat?

Mag je zakelijke e-mails bekijken van ex-werknemers?
Op grond van de wet mag u de zakelijke mail van (ex)werknemers inzien, míts u daar een gegronde reden voor heeft. Daarbij dient u een afweging te maken tussen het belang dat uw bedrijf heeft om de e-mail te bekijken en het privacybelang van de werknemer. Het verwijderen van belangrijke gegevens kan de continuïteit van de onderneming flink in de weg komen te staan. Ook kan het inzien van e-mail noodzakelijk zijn in het kader van de opvolging van de ex-werknemer. Deze omstandigheden wegen niet op tegen het belang van de werknemer de e-mail voor zichzelf te houden. Het bedrijfsbelang prevaleert dan ook boven het privacybelang van de werknemer. U mag de e-mail van (ex)werknemers dus bekijken. Ook staat de wet het toe dat u een back-up maakt van zakelijke e-mails en u mag het de werknemer zelfs verbieden e-mail te verwijderen. Zo voorkomt u dat belangrijke gegevens verloren gaan.

Mag je privé e-mails bekijken van ex-werknemers?
U dient het recht op privacy van de werknemer te respecteren. Om die reden is het lezen van privémail niet toegestaan. Het staat de werknemer dan ook vrij privéberichten uit de zakelijke inbox te verwijderen. Ook wanneer privémail binnenkomt nadat de werknemer is vertrokken, dient u deze ongeopend te laten.

Hoe lang mag zakelijke e-mails bewaren?
De privacywet stelt regels aan het bewaren van e-mail. Het basisprincipe is dat u de e-mails voor een ‘redelijke termijn’ termijn mag bewaren. Doorgaans betekent dit een bewaartermijn van maximaal 6 maanden. De termijn kan worden verlengd wanneer u daar een goede reden voor heeft, bijvoorbeeld bij een arbeidsconflict. Ook wanneer de werknemer toestemming geeft voor het langer bewaren van zijn e-mail is dit toegestaan**.**

Afspraken over e-mail
Het is raadzaam om afspraken over (het bewaren van) e-mail vast te leggen. Bijvoorbeeld in het arbeidsvoorwaardenreglement of in een ICT- en internetreglement. Zo weten u en de werknemer waar het op staat.

68. HR. Eigen Risico Drager

Wat zegt de Autoriteit Persoonsgegevens over de eigen risico drager?

- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-en-uitkering/mijn-privacy-bij-ziekte
- https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_de_zieke_werknemer.pdf

Bron:
https://www.uwv.nl/werkgevers/actueel/nieuwsbrief/2018/november/verbeterde-gegevensbescherming-met-machtigingsformulier-erd-zw.aspx

Hoe kun je als Eigenrisicodrager voor de Ziektewet je intermediairs machtigen?
Als eigenrisicodrager voor de Ziektewet moet werkgever sommige beslissingen verplicht voorleggen aan UWV. Is de uitvoer van verplichtingen overgedragen aan een intermediair, zoals een administratiekantoor, dan moet de intermediair gemachtigd worden om namens MAAS gebruik te maken van de UWV dienstverlening. U machtigt intermediairs met het formulier 'Machtiging eigenrisicodrager Ziektewet'. Om de machtiging(en) volledig volgens de Algemene Verordening Gegevensbescherming (AVG) te kunnen registreren, wordt in het formulier ook vastgelegd wie beslissingen mag aanvragen. Zo komt privacygevoelige informatie ook bij de aanvraag van beslissingen altijd op de juiste plaats terecht

Waar voor kun je de intermediair machtigen?
Met het UWV machtigingsformulier machtigt je maximaal 2 intermediairs voor UWV diensten. MAAS blijft wel verantwoordelijk voor de uitvoering. Machtiging voor:

- de inkoop van ondersteunende diensten en/of;
- het aanvragen van beslissingen.

Vereist UWV een verwerkersovereenkomst?
Ja, zorg voor een verwerkersovereenkomst. Omdat de gemachtigde persoonsgegevens voor MAA verwerkt, is MAAS verplicht met de gemachtigde een verwerkersovereenkomst te sluiten, op basis van de Algemene Verordening Gegevensbescherming (AVG). Bij controle kan het UWV om deze overeenkomst vragen. MAAS hoeft de verwerkersovereenkomst dus niet naar het UWV toe te sturen.

Hoe lag de gegevens bewaren bij ERD?

1. Als werkgever mag je verzuimgegevens tot maximaal twee jaar na afloop van een arbeidscontract bewaren. Dit geldt echter niet als je eigenrisicodrager voor de Ziektewet bent. In dat geval moet jij de gegevens over de ziekmelding vijf jaar bewaren, en de bedrijfsarts tien jaar. Voor het eigenrisicodragerschap voor de WGA mag je de gegevens tien jaar bewaren.
2. De bedrijfsarts mag dossiers van aanstellingskeuringen maximaal zes maanden bewaren. Andere medische dossiers mag hij maximaal vijftien jaar bewaren. Als er sprake is van een beroepsziekte, mag hij de gegevens langer dan vijftien jaar bewaren. Voor niet-medische dossiers geldt een bewaartermijn van maximaal twee jaar.
3. Re-integratiebedrijven mogen het medische deel van een re-integratiedossier maximaal vijftien jaar bewaren en het niet-medische deel niet langer dan twee jaar.

69. HR. Gezondheidsverklaring

Wat zegt de Autoriteit Persoonsgegevens over de gezondheidsverklaring?

4. Niets specifiek, wel over medische gegevens: https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/medische-gegevens-gebruiken-en-delen

Is het invullen van een gezondheidsverklaring toegestaan?
Het zomaar laten invullen van gezondheidsverklaringen door medewerkers is niet toegestaan op grond van privacy wet- en regelgeving, ook niet op basis van vrijwilligheid.

Waarom is het invullen van een gezondheidsverklaring toegestaan?
Een gezondheidsverklaring zorgt voor schijnveiligheid en is altijd een momentopname. Ziekteverschijnselen kunnen zich immers pas na invulling openbaren.
Conform de adviezen van het RIVM wordt van de werkgever verwacht dat bij bepaalde klachten (zoals neusverkoudheid, keelpijn, hoesten en koorts) de werknemer niet wordt ingezet. Het blijft belangrijk de richtlijnen van het RIVM te blijven volgen.
Toestemming vragen aan de werknemer om diens medische gegevens te mogen registeren, is geen goede oplossing. De Autoriteit Persoonsgegevens hanteert het standpunt dat in een werkgever–werknemer relatie toestemming niet vrijwillig tot stand is gekomen. Ook in de relatie met een opdrachtgever kan uw werknemer zich verplicht voelen om in te stemmen en is de toestemming niet vrijwillig tot stand gekomen. Bovendien kan toestemming door een werknemer altijd later worden ingetrokken.

Wat is een geneeskundige verklaring?
Een geneeskundige verklaring is een schriftelijke verklaring die een oordeel bevat over een patiënt en over de (medische) geschiktheid of ongeschiktheid van een patiënt om bepaalde dingen wel of niet te doen. Als behandelend arts mag je geen geneeskundige verklaring afgeven over eigen patiënten.
Geneeskundige verklaringen beoordelen of iemand in staat is om te werken, een auto te besturen, naar school te gaan, goed voor de kinderen te zorgen. Maar ook: is terecht een geboekte reis geannuleerd of heeft iemand recht op een parkeervergunning of aangepaste woonruimte?
https://www.knmg.nl/advies-richtlijnen/dossiers/geneeskundige-verklaring.htm

Wanneer is wel gezondheidsverklaring toegestaan door wet- en regelgeving?

1. Corona en vliegen: gezondheidsverklaring reizigers (Nederlands). Alle passagiers (van 12 jaar en ouder) die naar Nederland vliegen moeten een gezondheidsverklaring invullen. Soms kan dat digitaal. Soms moet u een formulier downloaden, printen en invullen. Dit verschilt per luchtvaartmaatschappij. Alleen met een gezondheidsverklaring kunt u aan boord gaan van het vliegtuig.
   https://www.rijksoverheid.nl/documenten/publicaties/2020/07/20/gezondheidsverklaring-reizigers-nederlands
2. CBR. Bent u gezond genoeg om een rijbewijs te halen of uw rijbewijs te verlengen? Dit beoordeelt het CBR met de Gezondheidsverklaring. Deze vult u zelf in. Op deze manier weet u zeker dat u veilig de weg op gaat. https://www.cbr.nl/nl/rijbewijs-houden/nl/gezondheidsverklaring.htm
3. Verzekeraar. Als je een levensverzekering of arbeidsongeschiktheidsverzekering wilt afsluiten, moet je meestal een gezondheidsverklaring invullen.
   https://www.verzekeraars.nl/publicaties/longreads/gezondheidsverklaring

4. Alleen in de vleesverwerkende sector heeft werkgever heeft het recht van zijn (toekomstige) werknemer een vormvrije gezondheidsverklaring te eisen in het kader van EU Verordening 852/2004. https://zoek.officielebekendmakingen.nl/stcrt-2017-13294.html en https://download.belastingdienst.nl/belastingdienst/docs/cao_vleessector_2019_2020_on6481z2ed.pdf

70. HR. Geheimhouding in contract

Wat zegt de Autoriteit Persoonsgegevens over de geheimhouding in contract?

- https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_verwerkersovereenkomsten.pdf

Geheimhoudingsverklaring verstandig?
Het is verstandig om medewerkers die veel met persoonsgegevens werken, nadrukkelijk te wijzen op hun verantwoordelijkheden. Maak met hen (aanvullende) geheimhoudingsafspraken. Dit kunt u doen in de arbeidsovereenkomst zelf, maar ook in een bijlage bij de arbeidsovereenkomst.

Voor welke functies geen aparte geheimhoudingsverklaring nodig?
Geheimhouding valt voor HR onder het beroepsgeheim. Voor OR-leden en FG wettelijke geheimhoudingsplicht.

Welke voorwaarden aan geheimhoudingsverklaring, bijvoorbeeld als addendum bij contract?
Bij een addendum op een arbeidscontract waarbij de werknemer geheimhouding opgelegd krijgt, en belooft netjes met persoonsgegevens om te gaan en alle documenten en dergelijke te retourneren aan het einde van het dienstverband. Dat betreft gewoon werkinstructies.

Mag een boeteclausule?
Boeteclausule mag niet. Een boete opleggen aan individuen, die handelen uit naam van een organisatie, voor het niet naleven van de AVG is verboden. Je mag deze personen ook niet aansprakelijk stellen voor het eventueel niet nakomen van het gestelde in de AVG.
Een (stevig) boetebeding is niet toegestaan: Dat is natuurlijk geen instructie, dat is een afspraak. Boetes mogen in arbeidscontracten worden opgenomen, maar dat is een tweezijdige vrijwillige keuze die je in zo'n contract maakt, en geen eenzijdig hier even tekenen. Een werkgever kan in principe niet eisen dat medewerker iets ondertekent, tenzij de handtekening uitsluitend dient als bewijs dat je iets gezien hebt. Een akkoord op een aanpassing van het arbeidscontract kan niet worden afgedwongen, behalve als het gaat om een kleine wijziging die in redelijkheid niet is te weigeren. Dat is natuurlijk niet aan de orde bij een boetebeding, omdat dit zozeer 100% in het nadeel van de werknemer is.
Persoonlijk aansprakelijk stellen voor de schade is evenmin toegestaan, de lat daarvoor ligt héél hoog en enkel dat medewerker een instructie negeert of de werkgever schade berokkent is nadrukkelijk bij lange na niet genoeg.

Relatie met AVG?
Bedrijfsgeheimen kunnen persoonsgegevens bevatten; informatie die direct of indirect te herleiden is tot een persoon. Uit de EU-richtlijn 2016/943, waarop het wetsvoorstel bescherming bedrijfsgeheimen is gebaseerd, blijkt dat deze geen afbreuk mag doen aan de privacywetgeving. Volgens overweging 34 en 35 van de betreffende richtlijn dient ook de privacy te worden gerespecteerd van personen wier persoonsgegevens deel uitmaken van het bedrijfsgeheim. Tijdens gerechtelijke procedures dienen bedrijfsgeheimen eveneens vertrouwelijk te worden behandeld, ook de persoonsgegevens die hier eventueel deel van uitmaken.

Lekken van bedrijfsgeheim tevens een datalek?
Het wetsvoorstel bescherming bedrijfsgeheimen staat naast de meldplicht voor datalekken in artikel 33 en 34 AVG; de regelingen hebben geen invloed op elkaar. Er kan zich een situatie voordoen waarbij een inbreuk op een bedrijfsgeheim tevens een datalek is. Persoonsgegevens, zoals namen

van personen die klant zijn of met wie wordt samengewerkt, kunnen immers deel uitmaken van een bedrijfsgeheim. Deze informatie kan uitlekken, en onbevoegden kunnen daar dan gebruik van maken.

Dan kan worden opgetreden tegen de inbreuk op het bedrijfsgeheim, maar dient tevens bij de Autoriteit Persoonsgegevens melding te worden gemaakt van het datalek (als dit een risico inhoudt voor de betrokkenen). Dat zal al gauw het geval zijn wanneer er bijvoorbeeld informatie uitlekt over met wie zij hebben samengewerkt aan een nieuw, nog onbekend product; of wie er allemaal klant zijn. Als er een hoog risico is voor betrokkenen, zal het ook aan hen moeten worden gemeld. Dit tenzij de gegevens bijvoorbeeld versleuteld/encrypted zijn en de sleutel niet is gelekt. Documenteer het lek dan wel intern, want het kan zijn dat later de sleutel uitlekt of de betreffende encryptiemethode wordt gekraakt, waardoor alsnog een melding aan de betrokkenen nodig is

Welke wetgeving voor bescherming bedrijfsgeheimen?
Op 23 oktober 2018 is de Wet bescherming bedrijfsgeheimen (Wbb) in werking getreden. Deze wet strekt tot implementatie van de Richtlijn bedrijfsgeheimen (2016/943/EU) en biedt houders van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) verschillende mogelijkheden om maatregelen te treffen tegen het onrechtmatig verkrijgen, gebruiken of openbaar maken van bedrijfsgeheimen.
Op 5 juli 2016 is de Richtlijn bedrijfsgeheimen (2016/943/EU) in werking getreden. De richtlijn heeft tot doel de regels inzake bescherming van bedrijfsgeheimen in de EU lidstaten te harmoniseren. De richtlijn moest voor 9 juni 2018 geïmplementeerd zijn in de Nederlandse wet- en regelgeving. Voor inwerkingtreding van de Wet bescherming bedrijfsgeheimen was er géén Nederlandse wetgeving die de bescherming van bedrijfsgeheimen waarborgde.
Op grond van de wet kan worden opgetreden tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken van bedrijfsgeheimen. Daarnaast hebben rechthebbenden op grond van de wet meer middelen gekregen om inbreuken op bedrijfsgeheimen te bestrijden. De wet voorziet verder in een definitie van bedrijfsgeheimen.

Voorheen deden werkgevers een beroep op een onrechtmatige daad (bv. wegens onrechtmatige concurrentie), dan wel wanprestatie of ‘goed werknemerschap’ (om de contractuele bescherming van het geheimhoudingsbeding in te roepen). De Wbb schept een basis om op te komen tegen onrechtmatige verkrijging van bedrijfsgeheimen, door bepaalde activiteiten als ‘onrechtmatig’ te bestempelen.

De Wbb voorziet niet in een uitputtende bescherming van bedrijfsgeheimen. Dat maakt het relevant om een geheimhoudingsbeding op te nemen waarin nader wordt gespecificeerd waarom bepaalde informatie geheim dient te blijven en wat de (financiële) consequenties zijn indien dat beding wordt geschonden. Bovendien dient aan het beding ook een boete te worden gekoppeld die hoog genoeg is om voldoende afschrikwekkend te zijn.
De Wbb vereist dat de houder van het bedrijfsgeheim redelijke maatregelen heeft getroffen om het bedrijfsgeheim te beschermen. Onder ‘redelijke maatregelen’ wordt mede verstaan het opnemen van geheimhoudingsclausules in arbeidsovereenkomsten. Dit maakt het van belang om in arbeidsovereenkomsten een geheimhoudingsbeding overeen te komen die in overeenstemming is met de Wbb. Verder kan worden gedacht aan fysieke (afschermende) of digitale beschermingsmaatregelen, zoals het versleutelen van gegevens (encryptie) of beveiligingssoftware. Denk ook aan de mogelijkheid om gegevens van een zakelijke telefoon (bij diefstal) te wissen, verzwaarde sloten op een rolkoffer, afscherming van privé-laptops en het voorkomen van heimelijke opnames van gesprekken.

71. HR. Nieuwe medewerker

Mogen persoonsgegevens van een nieuwe medewerker zoals voornamen, geboorteplaats, en het privé mailadres in de voorfase van de arbeidsovereenkomst verwerkt worden? Zo is in sommige gevallen het privé e-mailadres nodig om de link voor het vullen van de NAW-gegevens te sturen. Dit omdat er in dat stadium nog geen zakelijk mailadres bestaat. Mag dit?
Ja, dit mag, hetzij onder de grondslag 'noodzakelijk voor de uitvoering van de overeenkomst' hetzij onder de grondslag 'noodzakelijk voor het voldoen aan een wettelijke verplichting'.
Van een werknemer moeten wettelijk gezien immers bepaalde gegevens worden verwerkt, zoals een kopie van het legitimatiebewijs in het kader van de Wet op de loonbelasting. De overige gegevens, zoals het privé-emailadres of telefoonnummer, mogen worden verwerkt op grond van de onderliggende arbeidsovereenkomst. Vanzelfsprekend geldt dat enkel verwerkt mag worden wat noodzakelijk is.

Wij komen in de praktijk tegen dat nog wordt gevraagd om een kopie bankpas om na te gaan op welk rekeningnummer het salaris gestort mag worden. Deze kopie wordt als bijlage bij de mutatie gevoegd en opgeslagen. Mag dit (bijvoorbeeld in het kader van de wet WAS)? De techniek laat nu toe dat de medewerker zelf het bankrekeningnummer registreert, waarbij de verwerking rechtstreeks kan worden doorgevoerd in het personeelsinformatiesysteem.
Een werkgever is op grond van de Wet aanpak schijnconstructies (WAS) verplicht vast te stellen of het rekeningnummer daadwerkelijk bij de betreffende werknemer behoort. Er zijn verschillende manieren om dit vast te stellen:
1. De werknemer kan de bankpas tonen ter eenmalige identificatie.
2. De werkgever kan de werknemer een formulier voorleggen waarop de werknemer verklaart dat het bankrekeningnummer juist is.
3. De werkgever kan bepaalde gegevens van de bankpas afplakken (pasnummer en uitgiftedatum) en vervolgens een kopie maken en bewaren.

Is er een wettelijke grondslag is voor het vastleggen van privé bereikbaarheid gegevens anders dan op basis van toestemming?
Ja, hiervoor bestaat een grondslag, te weten ofwel 'noodzakelijkheid ten aanzien van een wettelijke verplichting' ofwel 'noodzakelijkheid bij de uitvoering van een overeenkomst'.
Adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens mogen worden verwerkt. De doeleinden waarvoor mag worden verwerkt, zijn hieronder weergegeven:

a. het geven van leiding aan de werkzaamheden van betrokkene;
b. de behandeling van personeelszaken;
c. het vaststellen en doen uitbetalen van salarisaanspraken;
d. het regelen van aanspraken op uitkeringen in verband met de beëindiging van een dienstverband;
e. de opleiding van betrokkene;
f. de bedrijfsmedische zorg voor betrokkene;
g. het bedrijfsmaatschappelijk werk;
h. de verkiezing van de leden van een bij wet geregeld medezeggenschapsorgaan;
i. de interne controle en de bedrijfsbeveiliging;
j. de uitvoering van een voor de betrokkene geldende arbeidsvoorwaarde;
k. het opstellen van een lijst van data van verjaardagen van betrokkenen en andere feestelijkheden en gebeurtenissen;
l. het verlenen van ontslag;

m. de administratie van de personeelsvereniging en van de vereniging van oud-personeelsleden;
n. het innen van vorderingen, waaronder begrepen het in handen van derden stellen van die vorderingen;
o. het behandelen van geschillen en het doen uitoefenen van accountantscontrole;
p. de overgang van de betrokkene naar of diens tijdelijke tewerkstelling bij een ander onderdeel van de groep, bedoeld in artikel 2:24b van het Burgerlijk Wetboek waaraan de verantwoordelijke is verbonden;
q. de uitvoering of toepassing van een andere wet.

Voor het vastleggen van de partnernaam grondslag bestaat mits de werknemer kiest voor een (samengestelde) achternaam die is opgebouwd uit de partnernaam. Is er echter een grondslag voor het vastleggen van partnergegevens zoals voorletters, geslacht en geboortedatum wanneer deze gegevens niet (meer) nodig zijn voor de pensioenaangifte (in het kader van de UPA)?
In het kader van het pensioen dienen bovenstaande gegevens inderdaad te worden verwerkt en minimaal zeven jaar te worden bewaard (op grond van artikel 169 Pensioenwet). Zodra verwerking op grond van deze wetgeving niet meer noodzakelijk is, is voor het verwerken van voorletters, geslacht en geboortedatum geen grondslag meer, mede gelet op het beginsel van opslagbeperking. Echter, gelet op pensioenaanspraken die doorgaans pas laat aan het licht komen, is het aan te raden de gegevens niet te snel te vernietigen. Mocht een onderneming daarnaast aanvullend nabestaandenpensioen aanbieden, dan is het in het kader van deze arbeidsvoorwaarde ook noodzakelijk om bovengenoemde gegevens te bewaren. Verder geldt te allen tijde dat enkel het noodzakelijke verwerkt mag worden. Voor al het overige bestaat alsdan geen grondslag voor verwerking.

Burgerlijke staat wordt nu uitgevraagd om te controleren of de keuze afdruknaam wettelijk gezien is toegestaan in relatie tot de burgerlijke staat. Tevens is voor deze opbouw gekozen omdat de medewerker in de praktijk vaak de keuze afdruknaam zal willen aanpassen als er een wijziging in de burgerlijke staat heeft plaatsgevonden. Is er een grondslag voor het uitvragen van de (ingangsdatum) burgerlijke staat?
Met betrekking tot de afdruknaam is naar mijn mening voldoende dat wordt gevraagd welke achternaam de werknemer als afdruknaam wenst te hanteren en dat wijzigingen hierin door de werknemer zelf worden doorgegeven. Het uitvragen van de burgerlijke staat is naar mijn mening niet noodzakelijk, en aldus ontbreekt een grondslag. Wanneer een pensioenregeling wordt gehanteerd door de werkgever kan verwerking van gegevens betreffende de burgerlijke staat noodzakelijk zijn voor de uitvoering van een wettelijke plicht, dan wel voor de uitvoering van de overeenkomst.

Mogen kindgegevens worden verwerkt?
Eén van de beginselen uit de AVG is het beginsel van doelbinding, inhoudende dat iedere verwerking gericht moet zijn op een bepaald doel. Wat is het doel van verwerking van de kindgegevens?
De geboortedatum van een kind kan bijvoorbeeld worden verwerkt ten behoeve van de toekenning van ouderschapsverlof. In het kader van minimale verwerking is verwerking van de naam van het kind niet zonder meer nodig, de geboortedatum is voor dat doel voldoende. Indien het toch gewenst is de naam van het kind te verwerken zonder grondslag, dan kan dit enkel en alleen op basis van toestemming van de ouder voor zover het kind jonger is dan 16 jaar. Ook hierbij geldt dat de toestemming vrij, actief en ondubbelzinnig moet zijn (zie hiervoor ook de vraag ten aanzien van de verwerking van gegevens om te kunnen waarschuwen in geval van nood).

Indien – zoals eerder besproken – een kind van een overleden werknemer recht heeft op nabestaandenpensioen, is (op dat moment) verwerking van alle gegevens die voor het uitkeren van dit pensioen noodzakelijk is, gerechtvaardigd.

Gegevens van een sollicitant mogen 4 weken dan wel maximaal 1 jaar bij toestemming worden bewaard. Echter, welke gegevens mogen verwerkt worden en welke zeker niet? Mogen/moeten de geboortedatum, het geslacht en een foto worden verwerkt?
Een mogelijke grondslag is 'toestemming van de betrokkene', dus hierop zou het verwerken van de foto gebaseerd kunnen worden. Dan moet wel sprake zijn van actieve, vrije en ondubbelzinnige toestemming, bijvoorbeeld via een e-mail. Van vrije toestemming van een sollicitant kan – net zoals in de arbeidsverhouding – echter niet snel uit worden gegaan vanwege de afhankelijkheidsrelatie. Daarnaast geldt het beginsel van opslagbeperking; enkel verwerken indien noodzakelijk. Het opslaan van de foto is niet noodzakelijk, derhalve is het raadzaam de foto op een cv bijvoorbeeld door te halen. Een werkgever kan eventueel tijdens een sollicitatiegesprek vragen om een legitimatiebewijs ter identificatie, echter dient dit legitimatiebewijs niet gekopieerd c.q. verwerkt te worden.

Welk naslagwerk ten aanzien van gegevensverwerking van de zieke werknemer kunnen wij raadplegen?
De Autoriteit Persoonsgegevens heeft eind 2016 een beleidsdocument gepubliceerd inzake gegevensverwerking van de zieke werknemer, zie hiervoor de onderstaande link.
Let wel, deze beleidsregels zijn opgesteld onder de Wbp, het is dus mogelijk dat een en ander onder de AVG gewijzigd wordt.
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_de_zieke_werknemer.pdf

Is de inzage van NAW-gegevens van medewerkers die niet ziek zijn of eerder waren gerechtvaardigd voor een arbodienst? Hierbij opmerkend dat deze toegang voor preventieve maatregelen benodigd kan zijn.
Arbodienstverleners moeten toegang krijgen tot persoonsgegevens van zieke werknemers voor de uitoefening van hun wettelijke taak op basis van de Arbeidsomstandighedenwet.
Wanneer de arbodienstverlener meer gegevens ontvangt van de werkgever dan noodzakelijk voor de uitoefening van de wettelijke taak en deze gegevens verwerkt, is de werkgever verwerkingsverantwoordelijke en de arbodienstverlener verwerker. Het is dan ook niet toegestaan om de arbodienstverlener meer gegevens te verstrekken dan noodzakelijk, zonder hierover afspraken te maken in een verwerkersovereenkomst. Zelfs al wordt een verwerkersovereenkomst afgesloten tussen werkgever en arbodienstverlener, betekent dit niet dat zomaar alle persoonsgegevens van het gehele personeelsbestand verwerkt mogen worden door de arbodienstverlener, want iedere verwerking dient een gerechtvaardigd doel te hebben.
Voor wat betreft het automatisch doorsturen van persoonsgegevens (inclusief BSN) van niet-zieke en nieuwe werknemers door de werkgever aan de arbodienstverlener geldt dat hiervoor geen wettelijke grondslag aanwezig is.
In een openbaar gemaakte brief aan OVAL (brancheorganisatie van arbodiensten) van 14 april 2016 heeft de Autoriteit Persoonsgegevens verduidelijkt dat er geen grondslag aanwezig is voor de arbodienst om het BSN van niet-zieke en nieuwe werknemers te verwerken. Voor overige persoonsgegevens van niet-zieke en nieuwe werknemers moet een afweging gemaakt worden of het al dan niet noodzakelijk is om de gegevens te verwerken. Dit zou alsdan in een verwerkersovereenkomst vastgelegd moeten worden. De conclusie is in ieder geval dat er geen wettelijke grondslag bestaat voor arbodienstverleners om NAW-gegevens van het gehele personeelsbestand van een werkgever te verwerken. Dit zal niet toegestaan zijn onder de AVG (en overigens ook niet onder de huidige wetgeving).

In diezelfde brief is de Autoriteit Persoonsgegevens ook ingegaan op de rechtmatigheid van verwerking met als doeleinde preventieve maatregelen. Ten aanzien van verwerken van het BSN-nummer bij een preventief spreekuur is volgens de Autoriteit Persoonsgegevens een wettelijke grondslag te vinden in artikel 8 van de Wet BSN in de zorg, omdat een preventief spreekuur onderdeel uit kan maken van de verlening van zorg. Voor andere persoonsgegevens (niet zijnde BSN) geldt dat enkel verwerkt mag worden wat noodzakelijk is. Denk hierbij aan een beperkt aantal gegevens die nodig zijn om de werknemer te kunnen bereiken (naam, adres en telefoonnummer).

Hoe kan een organisatie omgaan met persoonsgegevens die in het verleden zijn verwerkt op grond van (omgekeerde) toestemming, maar waarvan de daadwerkelijke toestemming zelf niet is vastgelegd (en dus naar alle waarschijnlijkheid niet 'actief' was)?
De AVG geldt voor alle verwerkingen die op dat moment 'voortbestaan'. Dit betekent dat het niet relevant is of de gegevens al in het systeem stonden, alle verwerkingen moeten voldoen aan de AVG. Kortom, als niet aantoonbaar is dat toestemming is verleend voor een verwerking (en er is geen andere grondslag aanwezig), dan moeten de gegevens verwijderd worden en moet toestemming worden gevraagd. Deze toestemming moet actief, vrij en ondubbelzinnig zijn. Bovendien mogen geen nadelige gevolgen zijn verbonden aan het niet geven van toestemming (bijvoorbeeld dat een overeenkomst zonder toestemming voor verwerking niet tot stand kan komen).

Welke maatregelen kan een organisatie treffen in het kader van de AVG wanneer de leidinggevende namens de medewerker persoonsgegevens vastlegt in het systeem? Zijn er tips hoe men dan kan omgaan met persoonsgegevens die op basis van toestemming worden verwerkt?
Het is niet relevant wie de persoonsgegevens daadwerkelijk verwerkt, zolang er maar sprake is van een grondslag voor verwerking. Een werknemer valt onder de verantwoordelijkheid van de verwerkingsverantwoordelijke, te weten de werkgever. Binnen de organisatie is wel van groot belang dat ook de werknemers zich ervan bewust zijn hoe om te gaan met persoonsgegevens. Daarom verdient het aanbeveling een goed intern privacy beleid op te (laten) stellen en dit beleid onder de aandacht te brengen bij het personeel.

Mag werkgever een privémailadres aan een externe partij verstrekken?
Werkgever verstrekt privémailadres aan een externe partij die mailt met fitnessaanbiedingen in verband met de bedrijfsfitness. Mag dit zomaar? Nee, een werkgever mag niet een privémailadres verstrekken aan derden.
Een werkgever mag zakelijke contactgegevens van een werknemer verstrekken aan derden als dat relevant is voor het werk. Dat is immers waar die contactgegevens voor bedoeld zijn. Verstrekking aan leveranciers en partners valt daar ook onder. Als een werkgever een bedrijfsfitnessregeling treft, dan zou je dus kunnen zeggen dat dit een partner is en die mag het personeel dan wijzen op die regeling en ze overhalen bij hen te komen sporten.
Meestal heeft een werkgever geen reden om privémailadressen te moeten hebben. Het kan zijn dat hij ze heeft om loonstroken heen te sturen, of hij krijgt ze uit correspondentie over bijvoorbeeld een ziekmelding. Maar dan moet het gebruik daarvan ook voor die doelen beperkt blijven. Verstrekken daarvan aan derden zou dus echt niet aan de orde moeten zijn.

Bron:

- https://www.aag.nl/wp-content/uploads/Memorandum.pdf Geraadpleegd 18-09-2019
- https://www.security.nl/posting/490423/Juridische+vraag%3A+Mag+mijn+werkgever+mijn+priv%C3%A9mailadres+aan+een+externe+partij+verstrekken%3F Geraadpleegd 27-09-2019

72. HR. Organigram

Wat zegt de Autoriteit Persoonsgegevens over een organigram?
…

Wat is nut en noodzaak van een organigram?
Een organigram of organogram is een schematische voorstelling van uw organisatiestructuur. Een organogram geeft inzicht hoe de organisatie feitelijk in elkaar zit:

- welke afdelingen zijn er
- wie is waar verantwoordelijk voor?
- waar liggen de bevoegdheden binnen uw bedrijf?

De organisatiestructuur is de basis voor de interne communicatie. En een organogram is een schematische weergave van deze bedrijfsstructuur.

Hoe worden de verhoudingen inzichtelijk gemaakt?
Een organisatiediagram maakt de verhoudingen binnen het bedrijf inzichtelijk. Hoe hoger iemand in het diagram staat getekend: hoe meer bevoegdheden de persoon in kwestie heeft en ook hoe meer verantwoordelijkheden.

73. HR. Overleden medewerker

Bronnen:

- https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacy-en-persoonsgegevens/wat-zijn-persoonsgegevens
- https://solv.nl/blog/post-mortem-wat-is-de-juridische-status-van-persoonsgege-vens-na-overlijden/
- https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_nl.pdf

Vallen gegevens van overleden personen onder de AVG?
De Algemene Verordening Gegevensbescherming (AVG) geeft aan dat een persoonsgegeven elk gegeven is over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Dat het om een natuurlijke persoon moet gaan, houdt in dat gegevens van overleden personen of van organisaties geen persoonsgegevens zijn.

Welke andere regelgeving over persoonsgegevens van overleden personen?
Anonimiseringsrichtlijnen rechtspraak. Het doel van deze richtlijn is aan te geven welke personen en gegevens geanonimiseerd moeten worden bij publicatie van een rechterlijke beslissing op rechtspraak.nl teneinde de privacy van deze personen te beschermen. *Onder natuurlijke personen worden tevens verstaan overleden personen. De gegevens van overleden personen worden geanonimiseerd. https://www.rechtspraak.nl/Uitspraken/paginas/anonimiseringsrichtlijnen.aspx

Kan ik het medisch dossier van mijn (overleden) familielid inzien?
Dit hangt er onder meer van af of uw familielid (boven de 16 jaar) in leven of overleden is. Voor deze situaties gelden verschillende regels.

- Inzage medisch dossier levend familielid: U kunt het medisch dossier van een levend familielid alleen inzien als deze hiervoor schriftelijk toestemming heeft gegeven. Is uw familielid wilsonbekwaam? Dan heeft u alleen recht op inzage als u de (wettelijk) vertegenwoordiger bent van uw familielid.
- Inzage medisch dossier overleden familielid: Is uw familielid overleden, dan heeft u in principe geen recht op inzage. U kunt wel inzage krijgen in (een aantal) medische gegevens als de overledene hiervoor toestemming heeft gegeven. U kunt ook inzage krijgen als u kunt aantonen daar een zwaarwegend belang bij te hebben. En er redelijkerwijs van kan worden uitgegaan dat uw overleden familielid geen bezwaar zou hebben gehad. Hiervan is bijvoorbeeld sprake als u een procedure wilt aanspannen tegen de zorgverlener of als u informatie wilt krijgen over een erfelijke aandoening.

Machtiging voor persoonsgegevens van een ander?
U heeft alleen rechten op eigen persoonsgegevens, tenzij u gemachtigd bent. In dat geval stuurt u het volgende mee met uw verzoek:

- Een machtiging (tenzij overleden persoon)
- Een kopie van uw legitimatiebewijs
- Een kopie van het legitimatiebewijs van de persoon waarvoor u gemachtigd bent.
- Als het gaat om persoonsgegevens van een overleden persoon moet u in plaats van een machtiging een uittreksel uit het overlijdensregister meesturen (ook wel akte van overlijden). En uw relatie met de betrokkene omschrijven.

Geeft de wettelijke verplichting tot het betalen van een overlijdensuitkering grondslag om de burgerlijke staat en partnergegevens uit te vragen?
Het betalen van een overlijdensuitkering is een wettelijke verplichting (artikel 7:674 BW) die veelal wordt ingevuld door de van toepassing zijnde collectieve arbeidsovereenkomst. De grondslag voor verwerking is dan ofwel de noodzakelijkheid om te voldoen aan een wettelijke verplichting ofwel de noodzakelijkheid voor de uitvoering van de overeenkomst (afhankelijk van de status van een cao). Indien geen sprake is van een echtgenote of relatiepartner, kan zijn bepaald dat de uitkering aan de kinderen van de overleden werknemer moet worden verstrekt. Verwerking van gegevens die hiervoor noodzakelijk zijn, zijn dan dus rechtmatig.

Oordeel rechtbank?
Het antwoord van de rechtbank is duidelijk: nee. De rechter oordeelt dat de op de AVG gebaseerde rechten bij uitstek persoonlijke rechten zijn, die alleen door de eiser zelf zijn in te roepen. Zij zijn niet vermogens- of familierechtelijk van aard en daarom niet voor overgang vatbaar, zoals bedoeld in artikel 4:182 lid 1 BW (erfopvolging onder algemene titel).

Overgang van rechten onder de AVG krachtens erfopvolging?
Nee.
Op grond van hoofdstuk 3 van de AVG hebben betrokkenen ten aanzien van hun persoonsgegevens verschillende rechten. Hieronder valt onder meer het recht op inzage, rectificatie of gegevenswissing. In overweging 27 van de AVG is bepaald dat de verordening niet van toepassing is op de persoonsgegevens van overleden personen. Wel wordt aan lidstaten de bevoegdheid gegeven nadere regels op te stellen ten aanzien van de uitoefening van privacy rechten van overleden personen. Bij de implementatie van de AVG heeft Nederland ervoor gekozen om geen nadere regels hierover op te stellen. Dit betekent dat in Nederland de AVG slechts van toepassing is op levende personen en hier door nabestaanden niet een beroep op kan worden gedaan.
In Nederland is de conclusie helder. De AVG is niet van toepassing op overleden personen en de AVG-rechten die aan betrokkenen toekomen zijn niet voor overgang vatbaar.

Hoe gaan andere Europese lidstaten hiermee om?
Aangezien de AVG ruimte biedt om nadere regels te stellen ten aanzien van de verwerking van persoonsgegevens van overleden personen, heeft een aantal lidstaten hier uitvoering aan gegeven. Zo treden in Bulgarije de erfgenamen in de plaats van de overledene om de AVG-rechten uit te oefenen. In Slowakije en Estland moeten nabestaanden toestemming verlenen voor de verwerking van persoonsgegevens van de overledene.
In Spanje hebben erfgenamen het recht op inzage, gegevens wissen en rectificatie van persoonsgegevens, tenzij verwijdering of correctie door de wet of de overledene verboden is. Italiaanse wetgeving geeft een ruime bevoegdheid om de rechten van de overledene te blijven uitoefenen. Het recht op inzage, rectificatie en het recht op gegevens wissen kan na het overlijden van de betrokkene uitgevoerd worden door iedereen die daar een belang bij heeft, of anderszins handelt ter bescherming van de overledene.
Frankrijk lijkt een duidelijk systeem te hebben ingericht om privacy ‘post mortem’ te regelen. Betrokkenen hebben de mogelijkheid om instructies op te stellen voor het beheer van hun persoonsgegevens na hun overlijden. Iedere betrokkene mag voor zijn of haar dood algemene of specifieke instructies opstellen omtrent de opslag, verwijdering of openbaarmaking van zijn of haar persoonsgegevens. Hetzelfde geldt voor de overerving van zijn of haar digitale activa. De overledene kan in de instructies een persoon aanwijzen die verantwoordelijk is voor de uitvoering hiervan. Indien er geen persoon is aangewezen maar er ook geen tegengestelde instructies zijn opgesteld kunnen de rechtsopvolgers van de overledene de instructies zelf uitvoeren. Een

verwerkingsverantwoordelijke dient zich aan deze instructies te houden en mag dit recht niet weg contracteren in algemene voorwaarden.

Oplossing voor deze lacune in de Nederlandse wet?
Hierboven is een (kort) overzicht geschetst van hoe Nederland en andere Europese jurisdicties omgaan met privacy 'post mortem'. In Nederland kunnen nabestaanden vooralsnog de privacy rechten van overledenen niet uitoefenen.

Het oordeel van de rechtbank in deze zaak is dan ook niet opmerkelijk. Nabestaanden van betrokkenen blijven (vooralsnog) aangewezen om geschillen over persoonsgegevens van overledenen via andere wegen op te lossen, bijvoorbeeld langs de lijnen van het verbintenissenrecht. Zo is het nabestaanden gelukt om toegang te verkrijgen tot een digitaal account van een overledene op basis van overgang van de overeenkomst die de overledene met de dienstverlener had gesloten. Toch zijn hiermee de rechten van overledenen nog niet genoeg geborgd, aangezien van een dergelijke onderliggende overeenkomst vaak geen sprake zal zijn. Deze lacune in de Nederlandse wetgeving kan leiden tot rechtsonzekerheid, zowel voor betrokkenen die geen duidelijkheid hebben over wat er met hun persoonsgegevens zal gebeuren wanneer zij komen te overlijden, als voor de nabestaanden. Het stellen van nadere regels over hoe hiermee moet worden omgegaan lijkt een logische stap in de huidige (digitale) samenleving.

Informatie over een overleden persoon?
Informatie over een overleden persoon kan ook iets zeggen over een levend persoon. Bijvoorbeeld bij een erfelijke ziekte. Dan zijn het persoonsgegevens van de levende persoon. En geldt daarvoor de AVG.
Dit kan bijvoorbeeld spelen bij een stamboom op internet. Staan daarin de ziekten vermeld waaraan mensen zijn overleden? Dan kan die informatie ook van toepassing zijn op de nabestaanden. En mag die informatie alleen op internet worden gepubliceerd als de nabestaanden daarvoor toestemming hebben gegeven.

Gegevens betreffende overledenen
Informatie over overleden personen wordt dus in beginsel niet beschouwd als persoonsgegevens waarop de regels van de richtlijn van toepassing zijn, aangezien overledenen civielrechtelijk geen natuurlijke personen meer zijn. Gegevens betreffende overledenen kunnen echter in bepaalde gevallen indirect nog enige bescherming genieten. Ten eerste is het mogelijk dat degene die voor de gegevensverwerking verantwoordelijk is, niet kan nagaan of de betrokkene nog leeft of inmiddels is overleden. Ook wanneer hij daartoe wel in staat is, kan het zijn dat gegevens over overledenen op dezelfde wijze worden verwerkt als gegevens betreffende levende personen. Aangezien de voor de verwerking verantwoordelijke, wat gegevens over levende personen betreft, volgens de richtlijn onderworpen is aan de verplichting tot bescherming van de gegevens, is het voor hem waarschijnlijk eenvoudiger om gegevens over overledenen eveneens volgens de regels voor gegevensbescherming te verwerken, in plaats van de twee soorten gegevens gescheiden te houden.
Ten tweede kan het zijn dat informatie over overledenen daarnaast ook betrekking heeft op levende personen. Het gegeven dat de overleden Gaia aan hemofilie leed, wijst er bijvoorbeeld op dat haar zoon Titius dezelfde ziekte heeft, aangezien deze wordt doorgegeven door een gen op het X-chromosoom. Wanneer informatie over overledenen dus tegelijkertijd levende personen betreft en daardoor als persoonsgegeven in de zin van de richtlijn geldt, geniet die informatie over een overleden persoon indirect de bescherming die de bepalingen van de richtlijn bieden.

24

Ten derde kan informatie over overledenen specifieke bescherming genieten op grond van andere regels dan de gegevensbeschermingswetgeving, die de grenzen afbakenen van wat sommigen “personalitas praeterita” noemen. De vertrouwelijkheidsplicht van medisch personeel eindigt niet met de dood van de patiënt. De nationale wetgeving inzake het portretrecht en ter bescherming tegen eerroof kan ook de nagedachtenis van de doden in bescherming nemen.

Ten vierde verzet niets zich ertegen dat een lidstaat de draagwijdte van de nationale wettelijke regeling houdende uitvoering van de bepalingen van Richtlijn 95/46/EG uitbreidt tot niet binnen de werkingssfeer daarvan vallende gebieden, voor zover geen enkele andere bepaling van gemeenschapsrecht daaraan in de weg staat, zoals het Hof van Justitie heeft opgemerkt16. Het is mogelijk dat een nationale wetgever de bepalingen van de nationale wetgeving inzake gegevensbescherming ook van toepassing verklaart op de verwerking van gegevens betreffende overledenen, indien een rechtmatig belang zulks rechtvaardigt17.

74. HR. Pandemie

Wat zegt de Autoriteit Persoonsgegevens over een pandemie?

- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona

Wat zeggen anderen?

- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona/privacy-corona
- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona/corona-op-de-werkvloer
- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona/veilig-thuiswerken-tijdens-corona

Welke invulling aan praktische vragen door pandemie?

Voor bedrijven brengt het virus verschillende uitdagingen met zich mee. Denk aan de verantwoordelijkheid van de werkgever om een veilige werkomgeving te garanderen aan alle werknemers en aan de uitdaging om de noodzakelijke continuïteit van de bedrijfsvoering te borgen. Bij het uitsturen van dit bericht hadden 130 werkgevers deeltijd WW aangevraagd voor hun werknemers en dit aantal zal de komende weken alleen maar toenemen. De invulling van wat praktische vragen lijken te zijn voor de werkgever, wordt voor een deel bepaald door de Algemene Verordening Gegevensbescherming (“AVG”). Tegelijkertijd heeft de werkgever allerlei verregaande verplichtingen op grond van de Arbeidsomstandighedenwet en is zorgvuldige actie geboden.
Deze actie kan bestaan uit het:

- introduceren van een helder beleid rond het coronavirus;
- in kaart brengen van mogelijke risico’s die werknemers kunnen lopen;
- treffen van maatregelen om risico’s te verkleinen;
- verstrekken van adequate informatie aan werknemers.

AVG & introduceren van beleid pandemie?

Het is voor werknemers en werkgevers prettig wanneer er duidelijke afspraken gelden binnen de organisatie. Vanwege de ontwikkelingen met en rond het coronavirus, vragen werknemers zich af of zij thuis moeten blijven als zij zelf in een risicogebied zijn geweest of (mogelijk) in aanraking met iemand die uit zo’n gebied komt. Werknemers kunnen de vraag stellen of zij thuis mogen blijven al dan niet om vanuit huis te werken als zij zich zorgen maken om hun gezondheid en wat de werkgever van hen verwacht als zij zelf besluiten om naar een besmet gebied af te reizen.
Er zijn verschillende situaties denkbaar waarbij een werkgever beleid zal moeten opstellen.

Werknemer drager van coronavirus?

Een werkgever kan niet zomaar werknemers thuis laten blijven of naar huis sturen. Dat kan de werkgever wel als duidelijk is dat een werknemer in één van de besmette gebieden is geweest, dan wel in aanraking met iemand anders die daar is geweest en/of wanneer een werknemer ziekteverschijnselen heeft. Ons advies is in dat geval om deze werknemers naar huis te sturen – of thuis te houden – en direct telefonisch contact op te nemen met de bedrijfsarts die anders dan de werkgever gerichte medische vragen kan stellen. Het is niet voor alle werknemers mogelijk om vanuit huis te werken vanwege de aard van het werk of omdat middelen ontbreken om dat vanuit huis te doen. Indien ondanks dat gegeven de werkgever de werknemer naar huis stuurt, is de werkgever in beginsel wel gehouden om het salaris door te betalen.

De Autoriteit Persoonsgegevens (“AP”) stelt weliswaar dat de werkgever geen conclusies mag trekken over individuele werknemers op basis van hun reisgegevens, maar de AVG belet werkgevers niet om dergelijke gegevens onder bepaalde omstandigheden te verwerken. Op grond van de AVG

mag de werkgever gegevens over reizen van werknemers verwerken als deze verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de werkgever of van derden. Dat is bijvoorbeeld het geval als deze informatie noodzakelijk is voor de werkgever om maatregelen te treffen ter bescherming van andere werknemers. De werkgever is op grond van de Arbeidsomstandighedenwet verplicht om gevaar zettende omstandigheden in kaart te brengen om vervolgens risicobeperkende maatregelen te kunnen treffen. Er zou daarom beargumenteerd kunnen worden dat het verwerken van reisgegevens van werknemers door de werkgever in dit kader noodzakelijk is mits de informatie wordt gebruikt voor het doel waarvoor het verzameld is.
Het is volgens de richtlijnen van de AP in beginsel niet toegestaan om werknemers te verplichten informatie over een mogelijke besmetting van het coronavirus in verband met bepaalde symptomen te verstrekken. De verwerking van dergelijke gegevens is namelijk onderworpen aan extra beperkingen. De AVG biedt in bepaalde omstandigheden ruimte voor de verwerking van gegevens over de aard en oorzaak van de ziekte van een werknemer, bijvoorbeeld in het geval dat dat noodzakelijk is ter bescherming van de vitale belangen van de werknemer. Denk aan een werknemer die een aandoening heeft waar collega's van op de hoogte moeten zijn. Er kan beargumenteerd worden dat kennis over het coronavirus, ook wanneer werknemers niet in een besmet gebied zijn geweest maar wel symptomen van het coronavirus vertonen, ook moet kunnen worden verzameld en gebruikt om maatregelen te kunnen treffen.
De AP stelt echter dat een werkgever, net zoals voor het coronavirus het geval was, niet mag vragen naar de aard en oorzaak van de ziekte wanneer de werknemer zich ziek meldt. Als de werknemer deze informatie op eigen initiatief deelt met de werkgever, mag de werkgever deze informatie ook niet registreren of gebruiken om een oordeel te vormen over de inzetbaarheid van die werknemer. Dat is de taak van de bedrijfsarts. Wij zien daarom een belangrijke rol voor de bedrijfsarts die zoals eerder opgemerkt wel vragen over medische informatie mag stellen aan de werknemer en die de werkgever vervolgens kan informeren over de inzetbaarheid van de werknemer.

Interne maatregelen tegen besmetting
Om het risico op besmetting zo klein als mogelijk te maken, hebben veel bedrijven ondertussen niet noodzakelijke reizen en bijeenkomsten geannuleerd. Wanneer reizen in het kader van werk onvermijdelijk is, dient de werkgever extra voorzorgsmaatregelen te treffen zoals extra instructies, aanvullende materialen en advisering zodat de werknemer het werk op een veilige manier kan blijven uitvoeren.

Bezorgde werknemers
Werknemers met een fragiele gezondheid kunnen door tussenkomst van een bedrijfsarts en zonder medische gegevens te (moeten) delen de werkgever, onder bepaalde omstandigheden, verzoeken om tijdelijk niet dan wel vanuit huis te werken. Indien thuis werken nodig en mogelijk is, dan houdt de werknemer aanspraak op het salaris. Dat geldt ook wanneer de bedrijfsarts adviseert dat de werknemer tijdelijk vanuit huis werkt. Indien thuiswerken niet kan en het risico op besmetting op of via het werk denkbaar is, dan geldt dat bepaalde werknemers een gerechtvaardigd belang kunnen hebben om tijdelijk betaald thuis te blijven. Het advies is om in alle gevallen de noodzaak en duur af te stemmen met de bedrijfsarts.

Reizende werknemers
Werknemers die met de kennis van nu besluiten om naar bepaalde gebieden af te reizen, lijken daarmee het risico van besmetting van zichzelf en voor anderen te vergroten. De werkgever kan de werknemer feitelijk niet verbieden om naar een dergelijk gebied af te reizen omdat het instructierecht van de werkgever niet zo ver gaat dat dit in mag grijpen in het privéleven van de werknemer. De werkgever kan de werknemer wel een reisadvies geven, rekening houdend met het reisadvies van het Ministerie van Buitenlandse Zaken ("BZ") en de werknemer sterk afraden om naar

landen waar een negatief reisadvies voor geldt, af te reizen. In het beleid van de werkgever kan worden bepaald dat wanneer een werknemer los van het reisadvies van BZ toch naar een besmet gebied reist, er een periode van minimaal twee weken ‘quarantaine’ geldt na terugkeer. Ons inziens kan van de werknemer uit dit voorbeeld gevraagd worden om extra vrije dagen op te nemen wanneer de terugreis wegens besmetting of quarantaine moet worden uitgesteld of als men eenmaal thuis geen werkzaamheden kan uitvoeren.

In kaart brengen van risico en treffen van maatregelen
Op grond van de Arbeidsomstandighedenwet moeten werkgevers de risico's van (de omstandigheden van) het werk in kaart brengen en verbeteringen voorstellen. Dit wordt vastgelegd in een RI&E: risico-inventarisatie & -evaluatie. De werkgever is verplicht om voorlichting en instructies te geven over deze risico's en over de maatregelen die daartegen genomen zijn. Situaties die gevaarlijk kunnen zijn worden in kaart gebracht om risico’s te verkleinen.
De werknemer moet veiligheidsinstructies van de werkgever opvolgen. Er is een speciale rol weggelegd voor de ondernemingsraad wanneer beleid dat geïntroduceerd wordt vanwege het coronavirus kan worden gezien als een wijziging van het bestaande beleid rond arbeidsomstandigheden. Over dit soort besluiten heeft de ondernemingsraad een instemmingsrecht. De tijd die nodig is om instemming te krijgen wordt mogelijk ingehaald door de feiten rond het virus en daarom wordt geadviseerd om de ondernemingsraad gezien de bijzondere omstandigheden tijdig te betrekken en te vragen om actief mee te denken en nieuw beleid te ondersteunen.

Informatie voor werknemers
De werkgever doet er goed aan om binnen de organisatie één vast contactpersoon aan te wijzen voor vragen over het werk en het coronavirus. Het ligt voor de hand om iemand van HR voor deze rol aan te wijzen. De werkgever kan via deze contactpersoon, werknemers actief voorlichten over het beleid van de organisatie vanwege (de ontwikkelingen van) het coronavirus. Deze contactpersoon kan ook de liaison zijn tussen werknemers en de bedrijfsarts en werknemers daarin de weg wijzen.

Werktijdverkorting en andere maatregelen
Niet alle werkgevers kunnen het werk vanuit huis laten uitvoeren en de stilstand van allerlei processen door het coronavirus raakt een snel groeiend aantal bedrijven. Werkgevers die kunnen onderbouwen dat vanwege het coronavirus het reguliere werk met minstens 20% afneemt, kunnen bij het Ministerie van Sociale Zaken en Werkgelegenheid een vergunning aanvragen voor werktijdverkorting en vervolgens bij het UWV een WW-uitkering aanvragen voor werknemers. Het aanvragen van de vergunning kan relatief eenvoudig via de website van de Rijksoverheid. Indien het coronavirus een dermate ernstige impact heeft op de bedrijfsvoering waardoor structureel omzet wegvalt, zal het voor sommige werkgevers noodzaak worden om arbeidsplaatsen te laten vervallen en is een procedure via het UWV onvermijdelijk.
Andere, minder vergaande, maatregelen die werkgevers kunnen treffen worden in sommige gevallen mede ingegeven door de toepasselijke cao en/of arbeidsvoorwaarden. Denk aan het opnemen van verlofuren of het over en weer uit- en inlenen van werknemers om de werkzaamheden beter te verdelen zonder extra loonkosten te maken. Deze bijzondere omstandigheden kunnen er ook toe leiden dat een werkgever sommige werknemers verzoekt om tijdelijk ander werk op een andere locatie uit te voeren.

Hoe zit het met privacy in geval van een pandemie?
Volgens de Autoriteit Persoonsgegevens (AVG) mag je als werkgever medische informatie niet vragen of vastleggen. Volgens de AVG heb je een grondslag nodig om persoonsgegevens te

verwerken (Artikel 6) en moet er bij de verwerking van medische gegevens sprake zijn van een uitzonderingssituatie benoemd in Artikel 9.
Een instantie mag persoonsgegevens verwerken

- Met toestemming van de betrokkene
- Als dit nodig is voor het uitvoeren van een overeenkomst
- Wanneer dit moet van de wet
- Als dit noodzakelijk is voor een vitaal belang voor de betrokkene of een derde
- In het kader van het uitvoeren van een taak van algemeen belang of handhaving van de openbare orde
- Als dit noodzakelijk is voor een gerechtvaardigd belang van die instantie, mits het privacybelang van de betrokkene niet prevaleert

Uitzonderingssituatie
Artikel 9 verbiedt het verwerken van medische gegevens, tenzij er sprake is van een uitzondering. Zo mag je medische gegevens verwerken met toestemming (a), als dit noodzakelijk is voor preventieve arbeidsgeneeskunde (h) of om redenen van algemeen belang op het gebied van de volksgezondheid (i).
Arts moet gevallen melden en mag mensen isoleren
Volgens de AVG mag de arts dus gegevens van een besmette werknemer verwerken, omdat de wet dit hem verplicht en omdat dit noodzakelijk is voor de volksgezondheid. In januari van dit jaar is namelijk een ministeriele regeling van de Wet publieke gezondheid (Wpg) aangenomen die een meldplicht introduceert voor het corona-virus (Covid 19). Indien een in Nederland werkzame (bedrijfs)arts corana-virus vermoedt of vaststelt, moet hij dit onmiddellijk melden aan een gemeentelijke gezondheidsdienst. Ook mag hij geïnfecteerde personen isoleren. Op basis van de Wpg mag een besmette persoon door de voorzitter van de veiligheidsregio worden verboden te werken en kan men voorschriften geven met betrekking tot terreinen en gebouwen.

Toestemming alleen in uitzonderlijke situaties
Ook toestemming biedt onvoldoende houvast. De AP zegt:
Er zijn enkele uitzonderlijke situaties denkbaar waarin de bedrijfsarts op grond van toestemming van de zieke werknemer gegevens over zijn gezondheid aan de werkgever kan verstrekken. Bijvoorbeeld als de werknemer zelf expliciet vraagt om de werkgever te laten weten dat hij epilepsie heeft en wat de werkgever moet doen in noodsituaties.
Dit zou op kunnen gaan voor Corona. De werknemer zou toestemming kunnen geven om directe collega's te informeren. Dat wil echter niet zeggen dat de werkgever de informatie mag bewaren.

Welk standpunt van de Europese toezichthouders (EDPD)?
Op 16 maart 2020 hebben de Europese toezichthouders, verenigd in de European Data Protection Board (EDPB), een verklaring gepubliceerd over de verwerking van gezondheidsgegevens in het kader van het coronavirus. De EDPB benadrukt dat de AVG geen belemmering vormt voor maatregelen in de strijd tegen het coronavirus. De AVG voorziet namelijk in wettelijke grondslagen om werkgevers in staat te stellen persoonsgegevens te verwerken in het kader van epidemieën, zonder dat daarvoor de toestemming van de betrokkene nodig is. Dit geldt bijvoorbeeld wanneer de verwerking van persoonsgegevens noodzakelijk is voor werkgevers om redenen van algemeen belang op het gebied van de volksgezondheid of om vitale belangen te beschermen (artikel 6 en 9 van de AVG) of om te voldoen aan een andere wettelijke verplichting. De EDPB lijkt dus meer ruimte te zien voor werkgevers.
Het probleem is dat sommige van door de EDPB genoemde uitzonderingen pas van toepassing zijn als deze in nationale wetgeving (de Uitvoeringswet AVG – UAVG) zijn opgenomen. Dit is voor Nederland niet altijd het geval, althans niet voor deze situatie. Ook bepaalt de AVG bijvoorbeeld wel

dat gezondheidsgegevens mogen worden verwerkt om vitale belangen te beschermen, maar pas indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven. Dat zal in deze situatie niet snel het geval zijn.
Toch kan je een aantal zaken nog wel doen

- Je mag je medewerker over zijn besmetting praten – je mag het alleen niet administreren voor eigen doeleinden. De privacywet gaat pas gelden als je medische informatie als organisatie gaat vastleggen in je eigen administratie.
- Je mag medewerkers ook vragen of ze op reis zijn geweest en waar en op basis daarvan voorzorgsmaatregelen nemen, zoals de medewerker verplichten thuis te werken.
- Je kan medewerkers instrueren over de symptomen en voorzorgsmaatregelen zoals handen wassen.
- Indien je een bedrijfsarts hebt kun je in samenspraak ook extra spreekuren en controles mogelijk maken.

75. HR. Personeelsdossier

Wat zegt de Autoriteit Persoonsgegevens over Personeelsdossier:
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-en-uitkering/personeelsdossiers

Bronnen:
https://www.awvn.nl/privacy-personeelsdossier/#
https://www.ploum.nl/recht-inzage-personeelsdossiers-avg/

Mag een kopie van het persoonlijke personeelsdossier opgevraagd worden?
Onder de AVG hebben medewerkers het recht om een kopie van het eigen personeelsdossier in een standaardformaat te ontvangen (bijvoorbeeld pdf).

Hoe is ESS beveiligd?
ADP services worden centraal gehost in Frankrijk, er is een back-up datacentrum in Spanje. De IT- en klantenservicemedewerkers werken vanuit Australië, Canada en India via beveiligde toegang op afstand.

Wie mag toegang hebben tot personeelsdossiers?
HRM-personeel, de direct leidinggevende en de medewerker zelf alleen voor zover dit noodzakelijk is om hun werk te doen.

Mag ik bijzondere persoonsgegevens van een medewerker opnemen in het dossier zoals godsdienst, gezondheid, etnische achtergrond, politieke gezindheid, seksuele geaardheid, lidmaatschap vakvereniging, strafrechtelijke veroordelingen?
Nee, al deze bijzondere persoonsgegevens mag u niet vermelden – tenzij sprake is van één van de uitzonderingen die in de wet genoemd zijn. Soms mag een gezondheidsgegeven wel worden vermeld, namelijk wanneer er sprake is van een vitaal belang. Als een werknemer op grond van bijvoorbeeld een cao-bepaling zijn vakbondscontributie declareert, mag u dit gegeven verwerken. U mag dit echter niet voor een ander doel gebruiken. U moet ook zorgen dat de gegevens zorgvuldig worden verwerkt en goed beveiligd zijn.

Mag ik gegevens over de gezondheid of ziekte van een medewerker vermelden?
Nee, dit is bij wet verboden en mag slechts gebeuren door personen die uit hoofde van hun beroep een geheimhoudingsplicht hebben.

Hoe ga ik om met het recht op inzage van de medewerker in zijn personeelsdossier?
De medewerker mag zijn gehele dossier inzien en een kopieën daarvan krijgen. U hoeft geen inzage te geven in notities en werkaantekeningen die uitsluitend bedoeld zijn voor intern overleg en beraad. Denk aan een intern memo over promotie of bonus. Dit is anders wanneer uitdrukkelijk is aangegeven dat die stukken deel uitmaken van het dossier van de medewerker.

Moet ik door de medewerker gevraagde correcties of aanvullingen doorvoeren?
Ja, u bent verplicht binnen vier weken foutieve persoonsgegevens te corrigeren of aan te vullen. Let wel: als een werknemer het niet eens is met bijvoorbeeld een disciplinaire maatregel of beoordeling, hoeft u die niet te corrigeren. De medewerker kan dan een eigen verklaring aan het dossier laten toevoegen.

Ben ik verplicht om aan een medewerker een kopie van zijn personeelsdossier te verstrekken?
Ja, dat bent u. Uitgezonderd notities en werkaantekeningen die uitsluitend bedoeld zijn voor intern overleg en beraad.

Volledige dossier ter beschikking stellen?
Onder de AVG moet de werknemer in beginsel een (digitale) kopie van zijn personeelsdossier ontvangen. Dit wil niet zeggen dat het volledige dossier altijd maar aan de werknemer ter beschikking moet worden gesteld. Bij een inzageverzoek van een werknemer is het altijd goed om eerst de volgende vragen te beantwoorden:

a. Is het verzoek buitensporig of ongegrond, bijvoorbeeld omdat de werknemer niet als doel heeft om zijn persoonsgegevens te controleren en eventueel aan te vullen, te wijzigen of te laten verwijderen
   - Zo ja: gemotiveerde afwijzing verzoek
   - Zo nee: door naar de volgende vraag
b. Welke gegevens worden opgevraagd?
   - Interne notities: niet ter inzage leggen
   - Stukken waardoor rechten of vrijheden van anderen (inclusief de werkgever zelf) worden beperkt: checken of wegstrepen mogelijk is; anders niet ter inzage leggens
   - Stukken die in principe niet onder a of b vallen: ter inzage leggen

Uiteraard hangt het van de concrete stukken in persoonsdossier af of HR deze volledig ter inzage dient te leggen.

Weigeren verzoek op inzage?
Een werkgever mag een verzoek op inzage van een werknemer weigeren of een redelijke vergoeding in rekening brengen, met name vanwege hun herhalend karakter, indien (art. 12 lid 5 AVG):

- een verzoek kennelijk ongegrond is, of;
- buitensporig is.

De bewijslast rust vervolgens bij de werkgever om de kennelijk ongegronde of buitensporige aard van het verzoek van de werknemer aan te tonen. Dit kan lastig zijn, omdat de werknemer geen reden hoeft op te geven voor het inzageverzoek. Vaak zal de werkgever echter wel een vermoeden hebben. Indien tussen werkgever en werknemer een conflict bestaat over vermeend disfunctioneren van de werknemer, kan het voor de hand liggen dat de werknemer zijn complete personeelsdossier opvraagt om ‘munitie’ te verzamelen in dit conflict. Het verzoek wordt dan voor een ander doeleinde gebruikt dan waarvoor het inzagerecht bedoeld is. De werknemer wil immers niet controleren welke (feitelijke) gegevens verwerkt worden en deze eventueel aanvullen, verbeteren, of wijzigen.
In de rechtspraak is ook uitgemaakt dat betrokkenen het inzagerecht niet mogen misbruiken voor een ‘fishing expedition’ naar zoveel mogelijk stukken waar toevallig hun persoonsgegevens op staan. Wij verwachten dat een dergelijke ‘fishing expedition’ ook onder de AVG kennelijk ongegrond zal zijn, wegens misbruik van bevoegdheid. Het blijft echter aan de werkgever om dit aan te tonen.
Overigens verwachten wij dat inzageverzoeken van werknemers niet vaak voor zullen komen. De werknemer heeft doorgaans al beschikking over de meeste gegevens. Indien een werknemer iets mist, iets wil weten of een wijziging wil doorgeven, zal hij uiteraard eerder een mailtje naar de HR-afdeling sturen dan dat hij een formeel inzageverzoek doet en vervolgens verzoekt om wijziging of aanvulling van gegevens. Dit kan ook een gezichtspunt zijn bij de beoordeling of een werknemer al dan niet een kennelijk ongegrond verzoek doet.

Mag ik voor het geven van kopieën kosten in rekening brengen?
Ja, u mag daarvoor een redelijke vergoeding in rekening brengen. Een werkgever die wordt geconfronteerd met een verzoek op inzage van een werknemer dient de werknemer in beginsel

kosteloos een kopie te verstrekken van de persoonsgegevens die van de werknemer worden verwerkt. Indien de werknemer om meerdere kopieën verzoekt kan de werkgever op basis van administratieve lasten een redelijke vergoeding in rekening brengen (art. 15 lid 3 AVG).

De medewerker vraagt welke persoonsgegevens in de organisatie over hem worden verwerkt. Hoe ga ik daar mee om?
U bent verplicht de medewerker binnen vier weken schriftelijk te informeren of en zo ja, welke persoonsgegevens over hem worden geregistreerd. De organisatie moet daarbij vermelden:

- of de organisatie zijn/haar persoonsgegevens gebruikt
- het doel van het gebruik
- om welke gegevens of categorieën het gaat
- de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt
- dat de betrokkene het recht heeft op rectificatie, beperking en het recht om bezwaar te maken tegen de verwerking van de persoonsgegevens
- dat de betrokkene het recht heeft om een klacht in te dienen bij Autoriteit Persoonsgegevens
- wat de herkomst is van de gegevens als deze gegevens niet bij de betrokkene zijn verzameld.

U moet ook zonder verzoek van een medewerker, uw medewerkers informeren over de manier waarop u met hun gegevens omgaat. Dit kan via de privacyverklaring van MAAS. MAAAS heeft hiermee het privacy beleid vastgelegd. Hiervoor geldt instemmingsrecht van de Ondernemingsraad op grond van de Wet op de Ondernemingsraden.

Anders gezegd: Onder de AVG dient een werkgever (een verwerkingsverantwoordelijke) aan een werknemer, die een inzageverzoek doet, te laten weten (art. 15 lid 1 AVG):

a. de verwerkingsdoeleinden (waarom bepaalde gegevens worden verwerkt);
b. de betrokken categorieën van persoonsgegevens (welke soorten persoonsgegevens u verzamelt);
c. indien van toepassing: aan welke organisaties u de persoonsgegevens doorgeeft (geldt ook voor gegevens die u doorgeeft aan organisaties in andere landen of internationale organisaties);
d. hoelang de persoonsgegevens worden bewaard, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
e. welke privacyrechten de werknemer heeft (het recht om persoonsgegevens te laten wijzigen, aanvullen of wissen, om te vragen minder persoonsgegevens te verwerken en om bezwaar te maken als persoonsgegevens worden verwerkt);
f. dat een werknemer het recht heeft een klacht in te dienen bij een toezichthoudende autoriteit (Autoriteit Persoonsgegevens);
g. indien van toepassing: van welke organisatie de persoonsgegevens zijn ontvangen wanneer de persoonsgegevens niet bij de werknemer worden verzameld;
h. indien van toepassing: op basis van welke logica een geautomatiseerd besluit over een werknemer wordt genomen.

Wat vormt de inhoud personeelsdossier binnen AVG?
Een personeelsdossier bevat in veel gevallen informatie over de persoon van de werknemer, waaronder NAW-gegevens, e-mailadres, telefoonnummer, salaris, arbeidsovereenkomst, paspoortnummer, maar onder andere ook beoordelings- en functioneringsgesprekken, medische gegevens (ziek- en herstelmeldingen), eventuele leaseovereenkomsten, en interne notities.

Doorgaans zal de werknemer over de meeste stukken zelf ook beschikken, zoals beoordelingen en salarisstroken.

Omvang recht op inzage binnen AVG?
In principe moet de werknemer dus een kopie ontvangen van de persoonsgegevens in het personeelsdossier. Een papieren kopie is niet verplicht: een gangbare elektronische vorm als een pdf'je is ook toegestaan. Indien mogelijk zou de werknemer ook kunnen inloggen op een online omgeving waar zijn personeelsdossier is opgenomen.
Er zijn een aantal beperkingen aan het inzagerecht. Ten eerste moet het om feitelijke gegevens gaan. In de rechtspraak is uitgemaakt dat interne notities van leidinggevenden, met daarin hun persoonlijke gedachten, niet verstrekt hoeven te worden. Deze stukken zijn immers bedoeld voor intern overleg en beraad, bijvoorbeeld als voorbereiding op de jaarlijkse beoordeling van werknemers.
Het recht op inzage mag verder geen afbreuk doen aan de rechten en vrijheden van anderen (art. 15 lid 4 AVG). Dit brengt met zich mee dat bij het verstrekken van een kopie van het personeelsdossier, de werkgever o.a. de privacyrechten van andere werknemers, bedrijfsgeheimen, IE-rechten etc. dient te borgen. Dit kan ertoe leiden dat namen van andere werknemers moeten worden weggestreept, bijvoorbeeld op een lijst van werknemers die momenteel een verbetertraject volgen wegens disfunctioneren. Ook het recht/de vrijheid van de werkgever om een goed personeelsbeleid te kunnen voeren, mag niet worden beperkt. Dit kan er toe leiden dat de werkgever bijvoorbeeld geen inzage hoeft te geven in een (voorlopig) overzicht van boventallige werknemers, terwijl de reorganisatie nog niet is aangekondigd.

Jurisprudentie?
- Werknemer heeft recht op inzage in het personeelsdossier: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBMNE:2018:3624
- Verbod op het gebruik maken van een in het kader van een arbeidsconflict opgesteld rapport is afgewezen, art. 17 AVG wissen van gegevens is geen absoluut recht https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2018:7398
- Verwerking door onderzoeksbureau van persoonsgegevens werknemer rechtmatig wegens gerechtvaardigd belang werkgever dat inbreuk op privacy rechtvaardigde; verzoek tot inzage afgewezen wegens gebrek aan belang https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2019:2166

76. HR. Pensioen

Wat zegt de Pensioenfederatie over Persoonsgegevens en pensioenfondsen:

- https://www.pensioenfederatie.nl/website/themas/pensioenuitvoering/privacybescherming
- https://www.pensioenfederatie.nl/website/publicaties/gedragslijn/gedragslijn-verwerking-persoonsgegevens-pensioenfondsen

Wat is de Gedragslijn Verwerking Persoonsgegevens Pensioenfondsen?
De Pensioenfederatie heeft samen met haar leden de Gedragslijn Verwerking Persoonsgegevens Pensioenfondsen gepubliceerd. Deze gedragslijn beschrijft hoe de pensioensector persoonsgegevens verwerkt. Pensioenfondsen maken hiermee aan alle deelnemers en pensioengerechtigden duidelijk hoe we omgaan met hun gegevens. Deze gedragslijn stemt overeen met bepalingen uit de AVG en wordt periodiek getoetst op wijzigingen in de Uitvoeringswet AVG en nieuwe interpretaties. Tijdens de ALV op 18 juni 2019 is de gedragslijn vastgesteld en Pensioenfederatie gaat ervan uit dat pensioenfondsen de gedragslijn naleven. De gedragslijn treedt vanaf 1 januari 2020 echt in werking.

Wat zegt AEGON over (beveiliging) persoonsgegevens:
https://www.aegon.nl/particulier/nieuws/gegevensbescherming-bij-aegon
https://www.aegon.nl/particulier/pensioen

Wat zegt Nationale Nederlanden over (beveiliging) persoonsgegevens:
https://www.nn.nl/Privacy.htm

Wat zegt Mijnpensioenoverzicht.nl over (beveiliging) persoonsgegevens:
https://www.mijnpensioenoverzicht.nl/faq

Mag een kopie van het persoonlijke pensioendossier opgevraagd worden?
Betrokkene is gerechtigd om het Pensioenfonds schriftelijk te vragen om een overzicht van de verwerkte Persoonsgegevens. Indien van toepassing zal het Pensioenfonds een volledig overzicht van de Persoonsgegevens verstrekken aan de Betrokkene. Als het Pensioenfonds geen Persoonsgegevens van de Betrokkene verwerkt, stelt het Pensioenfonds de Betrokkene daarvan ook op de hoogte.
Het Pensioenfonds verstrekt informatie aan de Betrokkene over welke Persoonsgegevens verwerkt worden, door eerst te vragen bij Betrokkene naar de redenen van het recht op inzage, om zodoende zijn belang beter te kunnen dienen.
Het Pensioenfonds kan om kostentechnische of andere redenen ervoor kiezen de wijze van invulling van het inzagerecht af te stemmen met betrokkene om een zo optimaal mogelijke invulling te geven en de opgevraagde gegevens beter af te stemmen op de aanleiding of de behoefte van Betrokkene.
Als het Pensioenfonds gebruik maakt van gedigitaliseerde Persoonsgegevens in een deelnemersportaal, kan het Pensioenfonds Betrokkene verwijzen naar de plaatsen op het portaal waar betrokkene de verwerkte Persoonsgegevens kan terugvinden. Tevens zal het Pensioenfonds aangeven of er nog op andere plaatsen Persoonsgegevens worden verwerkt en welk soort gegevens het betreft. Indien Betrokkene alsnog inzage wil hebben in de betreffende gegevens, heeft het Pensioenfonds de verplichting deze gegevens te leveren.

In stand houden oude pensioengrondslag verplicht bij demotie (kort) voor pensioen?
Als een werknemer binnen tien jaar voor zijn pensioen een andere functie met een lager salaris accepteert, is het wettelijk toegestaan om de oude pensioengrondslag te blijven hanteren. De werknemer gaat er door de demotie dan niet in zijn pensioen op achteruit. Het is voor uw onderneming niet verplicht om deze fiscale faciliteit aan te bieden. Het pensioen kan na demotie ook gewoon worden opgebouwd op basis van het werkelijke, lagere loon van de werknemer.

Pensioenuitvoerder moet pensioengevend loon weten?
Het pensioengevend loon is het salaris dat de werknemer daadwerkelijk verdient. Het gaat dan niet alleen over het bruto maandloon (dat meestal is gerelateerd aan een inschaling in de cao), maar ook de vakantiebijslag, de eindejaarsuitkering en bepaalde toeslagen tellen mee. Welke toeslagen precies in het pensioengevend salaris zitten, hangt af van de definities in de pensioenregeling. De bijtelling voor de auto van de zaak behoort in ieder geval niet tot het pensioengevend loon. Dit loonbestanddeel is in de wet uitgesloten. Onderneming moet aan de pensioenuitvoerder doorgeven wat het pensioengevend loon van de werknemer is. Op basis daarvan wordt bepaald hoeveel pensioen de werknemer mag sparen.

77. HR. Referenties vorige werkgever

Wat is de juiste werkwijze bij referenties geven?
Een werknemer heeft zijn ex-werkgever opgegeven als referent. De potentiële nieuwe werkgever neemt contact op met deze referent en krijgt onder andere negatieve referenties te horen. De instelling waar de werknemer gesolliciteerd heeft besluit vervolgens de werknemer niet aan te nemen. De werknemer stelt de referent aansprakelijk voor de schade.
Het Hof Arnhem-Leeuwarden oordeelt op 21 augustus 2018 dat als uitgangspunt heeft te gelden dat als een sollicitant in een sollicitatieprocedure zijn ex-werkgever aanwijst als referent, hij daarmee toestemming (in de zin van artikel 6 lid 1 sub a van de AVG) geeft om gegevens over zijn persoon en over zijn functioneren te verstrekken aan een ander. Deze informatie kan zowel positief als negatief voor de persoon in kwestie uitpakken. Wanneer een sollicitant bepaalde negatieve informatie van de referentie over zijn persoon of functioneren wil uitsluiten, dient hij dat volgens het Hof expliciet bij de referent aan te geven. De referent kan dan op zijn beurt een afweging maken of hij nog wel een referentie wil afgeven. Als voormalig werkgever zal hij immers een correct beeld van de betrokken persoon aan de potentiële werkgever moeten verstrekken. Het onthouden van informatie kan onzorgvuldig handelen en daarmee aansprakelijkheid voor de schade jegens de potentiële werkgever opleveren.
Als een referent besluit referenties te verstrekken betekent dit niet dat hij vervolgens alles over de ex-werknemer mag vertellen. De referent mag alleen informatie verstrekken die van belang is voor het functioneren van de sollicitant. De beantwoording van de vraag of sprake is van relevante informatie zal onder meer afhankelijk zijn van de inhoud van de gestelde vragen door de potentiële werkgever, de ernst van bepaalde gedragingen (zoals wangedrag), de aard van de functie, de betrokken belangen van derden, het tijdsverloop nadat zich bepaalde negatieve gebeurtenissen hebben voorgedaan en de eventueel getoonde verbetering. Het Hof kwam in deze zaak tot het oordeel dat de referent de belastende informatie over de ex-werknemer mocht doorgeven en dus niet onrechtmatig en ook niet in strijd met de AVG had gehandeld.
In deze zaak liep het dus goed af voor de instelling die de referenties had verstrekt. De zaak maakt echter nogmaals duidelijk dat zorgvuldig met het verstrekken van referenties moet worden omgegaan. De afweging moet worden gemaakt welke informatie noodzakelijk is en dus van belang is voor het functioneren van de ex-werknemer, maar er moet ook een waarheidsgetrouw beeld worden gegeven. Daarnaast kan het ook nog zo zijn dat in een overeenkomst ter beëindiging van de arbeidsovereenkomst tussen de ex-werknemer en de ex-werkgever is afgesproken dat partijen zich niet negatief over elkaar uit zullen laten jegens derden of dat positieve of neutrale referenties worden verstrekt. Als in dat geval voor de ex-werknemer negatieve referenties worden verstrekt, wordt in strijd met de overeenkomst gehandeld.
Als u wordt benaderd voor referenties is het verstandig om niet direct die referenties te verstrekken maar eerst te bepalen welke informatie kan worden gedeeld. Soms weet u niet eens dat u als referent bent opgegeven en kunt u overvallen worden door een (telefonisch) verzoek van een potentiële werkgever. Laat u niet verleiden om in het telefoongesprek direct informatie te verstrekken. Dat is natuurlijk anders als u zich alleen in positieve zin over de werknemer kunt uitlaten, maar als u niet (geheel) positief bent over de ex-werknemer doet u er verstandig aan om de potentiële werkgever te vragen het verzoek om referenties en de specifieke vragen te mailen, en eventueel aan de ex-werknemer te vragen of het klopt dat u als referent bent opgegeven, zodat vervolgens een zorgvuldige afweging kan worden gemaakt. Bron: https://www.privacy-web.nl/pagina/pot-jonker-advocaten

78. HR. PSO ladder

PSO-Nederland en TNO hechten veel waarde aan het borgen van de Privacy in relatie tot de PSO. Voor gebruikers van de PSO en klanten van PSO-Nederland staan daarbij de volgende zaken centraal:

1. Bij het aanmaken van een MijnPSO account dient MAAS als gebruiker akkoord te gaan met (het lezen van) PSO Gebruikersvoorwaarden.
2. Daarnaast is er een Handreiking Privacy compliance tot stand gekomen om nadere informatie te geven over hoe MAAS privacy compliant gebruik kan maken van de PSO: PSO TNO Handreiking privacy compliance 2018: https://www.pso-nederland.nl/uploads/pso/PSO%20Nederland%20PDF/PSO%20TNO%20handreiking%20compliance%20Privacy%20april%202018.pdf
3. Daarnaast is er een Privacystatement opgesteld. In PSO Privacystatement uitgelegd hoe PSO omgaat met (persoons)gegevens: https://www.pso-nederland.nl/over-de-pso/avg

Wie levert info voor audit treden ten behoeve van de PSO ladder?
Voor de PSO ladder dient HR alleen aantal op te geven, aantal uren etc. Ten aanzien van de tredes moet je een aantal medewerkers in dienst hebben en dat geeft dit overzicht aan.
Doel is om een trede hoger te komen en daarvoor moeten we naar 33 SROI medewerkers. Dit is alleen voor PSO ladder en niet t.b.v. contracten met opdrachtgevers.

Welke eisen aan loonsom?
De eis dat een specifiek % van de werknemers binnen één van de doelgroepen van het artikel valt moet op een substantiële manier zijn ingevuld. Kortlopende tijdelijke contracten en nul-urencontracten horen daar dus niet bij. Een werkgever kan aan de hand van bijvoorbeeld de verloonde uren of de loonsom aantonen een substantiële invulling te geven aan de %-eis.

Percentage van de loonsom (minimaal 5%) welke door MAAS geïnvesteerd wordt in het bieden van werkplekken voor mensen met een afstand tot de arbeidsmarkt?
De kosten die ingezet worden t.b.v. SROI zijn gesplitst tussen medewerkers in dienst en via Teamwerk.
De facturen hiervoor worden door de planning gecontroleerd. Van Heilige Boontjes ontvangt HR geen factuur of iets dergelijks. HR afhankelijk ben van Kariem (operators bij een opdracht), Marion (loonsom) en finance (gefactureerde uren via Teamwerk).

Vereiste SROI % van loonsom bij arbeidsintensieve opdrachten?
De opdrachtnemer is verplicht bij arbeidsintensieve opdrachten, opdrachten met een loonsom van minstens 30% van de totale opdrachtwaarde, minimaal 5% van de opdrachtwaarde excl. BTW te besteden aan invulling van zijn social return verplichting.

Vereiste SROI % van loonsom bij arbeidsextensieve opdrachten?
Wanneer de opdracht arbeidsextensief is, wanneer de loonsom minder is dan 30% van de totale opdrachtwaarde, wordt 2% van de opdrachtwaarde excl. BTW als social return verplichting opgenomen.

Wat is het PSO 30+ certificaat?
Het PSO 30+ certificaat erkent organisaties die minimaal aan de gestelde kwantitatieve eisen van artikel 2.82 van de Aanbestedingswet voldoen.
Let op! Het toepassen van voorbehouden opdrachten o.b.v. artikel 2.82 van de Aanbestedingswet door (semi-) publieke opdrachtgevers betekent iets ander dan het toepassen van Social return bij

aanbestedingen (met de PSO). Voor de toepassing van artikel 2.82 van de Aanbestedingswet (voorbehouden opdrachten) heeft de Cedris voor publieke diensten en opdrachtgevers zoals gemeenten een Handleiding Sociaal aanbesteden met artikel 2.82 laten ontwikkelen door Van Doorne advocaten.

Wat betekent artikel 2.82 van de Aanbestedingswet?
Voorheen konden opdrachten uitsluitend voorbehouden worden aan SW-bedrijven op basis van het percentage doelgroep. In de nieuwe Aanbestedingswet is het percentage doelgroep voor voorbehouden opdrachten van 50% verlaagd naar 30% en opengesteld voor alle organisaties. Op 1 juli 2016 is de herziening van de Aanbestedingswet van kracht geworden. Aanbestedende diensten, zoals gemeenten, kunnen ervoor kiezen aanbestedingsprocedures voor te behouden aan zogenaamde 'sociale' bedrijven die aan de voorwaarde van dit wetsartikel voldoen.
Dat betekent dat aan deze aanbestedings-procedures alleen kan worden deelgenomen door sociale werkplaatsen en ondernemers die de maatschappe-lijke en professionele integratie van gehandicapten of kansarmen tot hoofddoel hebben, of de uitvoering ervan voorbehouden in het kader van programma's voor beschermde arbeid. Belangrijke voorwaarde daarbij is dat ten minste 30% van de werknemers van deze sociale werkplaatsen, ondernemingen of programma's gehandicapte of kansarme werknemers is.

79. HR. Rijbewijs

Bevat het rijbewijs een BSN-nummer?
Vanaf 1 oktober 2006 geeft de Rijksdienst voor het wegverkeer rijbewijzen uit in creditcard formaat. Deze bevatten een barcode. Sinds 19 januari 2013 zitten er in nieuwe uitgegeven rijbewijzen naast een barcode ook een verkorte MRZ, waarin geen BSN is opgenomen. Vanaf 14 november 2014 bevat het rijbewijs een MRZ, een Quick Response (QR)-code en een RFID-chip. Op de RFID-chip staan de houdergegevens en het BSN in aparte datagroepen, respectievelijk DG1 en DG11. Een rijbewijs dat vanaf 26 mei 2018 is afgegeven is heeft een nieuwe chip. Als het beeldmerk op de achterkant van het rijbewijs staat dan heeft het rijbewijs een extra functie waardoor het rijbewijs geschikt is om in de toekomst te gebruiken om online in te loggen via DigiD op websites van overheid, zorg en pensioenfondsen. Deze manier van inloggen geeft extra zekerheid over de identiteit van degene die inlogt en maakt het mogelijk zeer vertrouwelijke informatie online aan te bieden. Op de achterkant van het rijbewijs staat een beeldmerk. Hieraan kunt u zien dat het rijbewijs geschikt is om in de toekomst te gebruiken om online in te loggen via DigiD.

Waar vind ik mijn burgerservicenummer (BSN) op mijn rijbewijs?
U vindt uw burgerservicenummer (BSN) op de achterkant van uw rijbewijs, linksboven. Achter het BSN staat het rijbewijsnummer (gescheiden door een /). Op onderstaande afbeelding is het BSN (gevolgd door rijbewijsnummer) rood omcirkeld.

Welke echtheidskenmerken?
https://www.rdw.nl/particulier/voertuigen/auto/het-rijbewijs/over-het-rijbewijs/echtheidskenmerken-rijbewijs

Rijbewijs identiteitsbewijs?
In Nederland is het rijbewijs sinds 1 januari 2005 tevens een identiteitsdocument.
https://www.rdw.nl/particulier/paginas/campagne-laat-u-niet-zomaar-kopieren

Op basis van welke grondslag mag HR kopie rijbewijs conform de AVG verwerken?
Grondslag gerechtvaardigd belang. Kopie rijbewijs in het personeelsdossier en degene die de medewerker aanneemt zou voor deze bescheiden moeten zorgen alvorens de autosleutels overhandigd worden. Nieuwe auto's als eerste door Fleet Manager uitgegeven. Vervolgens bij personeelsmutaties veel met de wagens geschoven. Wijzigingen van berijder over het algemeen doorgegeven aan de Fleet Manager door de lijnfunctionarissen, maar lang niet altijd. Soms zijn het zelfs vakantiekrachten waar auto's aan beschikbaar gesteld worden.

Worden door MAAS persoonsgegevens van strafrechtelijke aard verwerkt ten aanzien van rijbewijzen?
Ja, volgens de MAAS Autoregeling dient: *"… intrekking van het rijbewijs onmiddellijk te worden gemeld aan de Fleetmanager. Deze regeling geldt eveneens als het rijbewijs zou zijn ingevorderd voor een bepaalde termijn.*
Persoonsgegevens van strafrechtelijke aard zijn: *"… persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen als bedoeld in artikel 10 van de (AVG) verordening, alsmede persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag"*

In welke situaties is rijden strafbaar voor een specifieke medewerker of familielid en is daarmee sprake van strafrechtelijke persoonsgegevens?
Het rijden tijdens de ontzegging van de rijbevoegdheid of nadat het rijbewijs ongeldig is verklaard dan wel de geldigheid is geschorst, is strafbaar gesteld in artikel 9 Wegenverkeerswet (WVW):

- Rijden tijdens de ontzegging van de rijbevoegdheid (lid 1)
- Rijden terwijl rijbewijs voor die categorie ongeldig is verklaard (lid 2)
- Rijden nadat op grond van artikel 130 WVW de overgifte van het rijbewijs is gevorderd (lid 4)
- Rijden nadat de geldigheid van het rijbewijs is geschorst (lid 5)
- Rijden nadat het rijbewijs is ingevorderd op grond van artikel 164 WVW, wegens alcohol, snelheid, gevaarlijk rijgedrag (lid 7)
- Rijden nadat de inlevering van het rijbewijs is gevorderd op grond van de Wet Administratiefrechtelijke Handhaving Verkeersvoorschriften (WAHV), in verband met openstaande boetes (lid 8)
- Rijden tijdens alcoholslotprogramma in ander motorrijtuig dan waar alcoholslot is ingebouwd, en waarvan kenteken met code 103 op het rijbewijs staat vermeld en/of rijden terwijl ander in het alcoholslot heeft geblazen (lid 9)

Op basis van welke grondslag mag de Fleetmanager strafrechtelijke persoonsgegevens (ontzegging van de rijbevoegdheid, rijbewijs ongeldig verklaard, geldigheid rijbewijs geschorst) conform de AVG verwerken?
De verwerking van bijzondere en strafrechtelijke persoonsgegevens is in principe verboden. Tenzij MAAS zich kan beroepen op een specifieke wettelijke uitzondering én op 1 van de 6 grondslagen voor het verwerken van 'gewone' persoonsgegevens:
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken#wanneer-mag-u-strafrechtelijke-persoonsgegevens-verwerken-6342
Persoonsgegevens van strafrechtelijke aard alleen worden verwerkt voor zover dit krachtens de artikelen 32 en 33 van de Uitvoeringswet Algemene verordening gegevensbescherming is toegestaan.
MAAS gebruikt hiervoor de uitzonderingsgrond, artikel 33., lid 2b:
Persoonsgegevens van strafrechtelijke aard mogen worden verwerkt door de verwerkingsverantwoordelijke die deze gegevens ten eigen behoeve verwerkt: … a. ter beoordeling van een verzoek van betrokkene om een beslissing over hem te nemen of aan hem een prestatie te

leveren; of b. ter bescherming van zijn belangen, voor zover het gaat om strafbare feiten die zijn of op grond van feiten en omstandigheden naar verwachting zullen worden gepleegd jegens hem of jegens personen die in zijn dienst zijn.

Waar wordt ontzegging van de rijbevoegdheid nog meer geregistreerd?
Daarvan melding gemaakt in de databanken van de Stichting Centraal Informatie Systeem (CIS) CIS. Dit gebeurt als de politierechter u een ontzegging van de rijbevoegdheid oplegt, bijvoorbeeld vanwege het gebruik van te veel alcohol in het verkeer. Uiteraard kan dit type Stichting CIS-vermelding ook door andere oorzaken ontstaan. De Stichting Centraal Informatie Systeem (CIS) is een organisaties van en vóór verzekeraars en hun gevolmachtigden. De stichting houdt gegevens bij van personen en bedrijven, zodat verzekeraars risico's beter kunnen inschatten. Een vermelding bij het CIS gaat dus over aanwezigheid in de databanken bij deze stichting. Eenmaal geregistreerd kan dat verschillende gevolgen hebben, afhankelijk van het type melding.

- https://www.stichtingcis.nl/nl-nl/regelgeving.aspx
- https://www.stichtingcis.nl/nl-nl/privacystatement.aspx
- https://www.stichtingcis.nl/nl-nl/consumenten/duurregistraties.aspx
- https://www.advocatenkantoorphea.nl/verzekeringsrecht/stichting-cis-de-registraties-uitgelegd/

Wanneer is rijbewjis identificatie bewijs ?
In Nederland is het rijbewijs sinds 1 januari 2005 ook een identiteitsdocument en inmiddels is het rijbewijs het meest gebruikte identiteitsdocument. U kunt het rijbewijs bijvoorbeeld gebruiken voor het afsluiten van een huurcontract of telefoonabonnement. Het rijbewijs is echter niet in alle situaties als identiteitsbewijs toegestaan. In het onderstaande overzicht ziet u wanneer u welk identiteitsbewijs mag gebruiken.

Situatie	Paspoort / Nederlandse identiteitskaart	Rijbewijs / bromfietsrijbewijs (categorie AM)
bij identiteitscontrole door politie, marechaussee en toezichthouders	ja	ja
bij de Belastingdienst	ja	nee
bij geldzaken	ja	ja
bij aanvraag van een burgerservicenummer (voorheen sofinummer)	ja	nee
bij de notaris	ja	ja
bij het aanvragen van een uitkering	ja	nee
bij in dienst treden bij nieuwe werkgever	ja	nee
op het werk	ja	ja
in de zorg	ja	ja
bij zwartrijden in het openbaar vervoer	ja	ja
bij binnenlands vreemdelingentoezicht	ja	nee
bij het bezoeken van bijvoorbeeld een voetbalwedstrijd	ja	ja
bij het stemmen bij verkiezingen	ja	ja

In tegenstelling tot een Nederlandse identiteitskaart of een nationaal paspoort is een rijbewijs niet gebonden aan een nationaliteit. Een buitenlander die in Nederland woont, kan hier examen doen en daarmee in het bezit komen van een rijbewijs.

Hoe voorkom ik identiteitsfraude met het rijbewijs?
https://www.rdw.nl/particulier/paginas/campagne-laat-u-niet-zomaar-kopieren

80. HR. Screening

Wat zegt de Autoriteit Persoonsgegevens over screening?
Zie:

- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-uitkering/screening
- https://www.autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten
- https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/politie-en-justitie/particuliere-recherche

Op basis van welke grondslag mag screening een Verklaring Omtrent het Gedrag VOG delen?
Grondslag is wettelijke verplichting in het kader van de uitvoering van een overeenkomst. Voor de opsporing, vervolging en afdoening van strafbare feiten verzamelt justitie allerlei persoonsgegevens. Ook voor het afgeven van een Verklaring Omtrent het Gedrag (VOG) worden persoonsgegevens verwerkt. De *Wet justitiële en strafvorderlijke gegevens (Wjsg)* regelt het verwerken van justitiële gegevens (in persoonsdossiers) en de verklaring omtrent het gedrag. De wet regelt ook de verwerking van strafvorderlijke gegevens. De Autoriteit Persoonsgegevens ziet toe op de verwerking van justitiële gegevens op basis van deze wet.

81. HR. Smoelenboek

Wat zegt de Autoriteit Persoonsgegevens over een smoelenboek?

- https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-en-uitkering/verstrekken-van-personeelsgegevens
- https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens

Is het zo dat als wij een smoelenboek willen maken wij expliciet toestemming van de medewerker moeten hebben om zijn/haar foto te gebruiken?

Ja, dat mag alleen met expliciete en vrijwillige toestemming en met duidelijk uitleg waarvoor werkgever toestemming vraagt. En wat de gevolgen zijn als medewerker toestemming geeft. Geeft medewerker geen toestemming? Dan mag dit geen negatieve gevolgen voor medewerker hebben. Als werkgever moet je kunnen bewijzen (schriftelijk in personeelsdossier vastleggen dus) dat je toestemming van de werknemer hebt ontvangen.

Let op:

- Toestemming wordt door de Autoriteit Persoonsgegevens niet gauw als een geldige reden gezien voor verstrekking van gegevens gezien. Dat komt omdat medewerker afhankelijk is van werkgever (arbeidsrelatie).
- Een smoelenboek op de website zelfs met toestemming niet geoorloofd. Smoelenboek mag alleen via een intranet toegankelijk zijn.
- Omdat uit een foto een ras of etnische afkomst valt af te leiden, is dat een bijzonder persoonsgegeven, volgens de Hoge Raad. Portretten zijn eigenlijk altijd bijzondere persoonsgegevens. Alleen al omdat er ras en etniciteit uit af zijn te leiden en eventueel zelfs wat gezondheidsgegevens, zoals een leeftijd of misschien medische gegevens omdat aan de foto een ziekte of beperking valt af te leiden, bijvoorbeeld om dat er een bril te zien is. Een hoofddoekje, keppeltje of ketting met kruisje kunnen het geloof verraden. Een organisatie mag geen bijzondere persoonsgegevens gebruiken, tenzij daarvoor in de wet een uitzondering is of de of de betrokkene uitdrukkelijk toestemming heeft gegeven voor de specifieke (en géén andere) verwerking.

82. HR. Sollicitaties

Bron: https://www.awvn.nl/privacy-arbeidsrelatie-sollicitatie/

Mag ik als werkgever een sollicitant vragen naar zijn gezondheid of zijn ziekteverzuim bij de vorige werkgever?
Nee, u mag hier vanwege de privacy van de sollicitant niet naar vragen. Als hij een ziekte of beperking heeft waarvan hij weet dat hij daardoor niet zonder meer in staat is de functie te verrichten conform de functie-eisen, dan dient de sollicitant dit wel uit zichzelf aan te geven. Denk bijvoorbeeld aan onderdelen van de functie die hij vanwege die ziekte of beperking niet kan uitvoeren.

Mag ik de sollicitant vragen of zij zwanger is?
Nee, u mag slechts vragen stellen over aspecten die voor de functie of functievervulling relevant zijn. Zie ook het antwoord op de vorige vraag. De sollicitant hoeft uit eigen beweging ook niets te zeggen over een eventuele zwangerschap. U mag ook niet informeren naar een eventuele kinderwens.

Is de sollicitant verplicht informatie te geven over een ziekte die hij heeft?
Nee, tijdens het sollicitatietraject mag de werkgever geen vragen stellen over de gezondheid van de sollicitant. Maar wanneer een sollicitant weet of behoort te weten dat hij om fysieke of psychische redenen de functie waarop hij solliciteert niet zonder meer conform de functie-eisen kan vervullen, is hij wel verplicht daarover uit zichzelf mededeling te doen. De werkgever kan dan samen met de sollicitant bekijken of dit een belemmering is om hem aan te nemen en of deze weg te nemen zijn door aanpassingen of hulpmiddelen.

Wat kan ik doen als achteraf blijkt dat de medewerker een ziekte heeft verzwegen die hem ongeschikt maakt voor de functie?
Dit kan, afhankelijk van de situatie, een reden opleveren voor een beëindiging van de arbeidsovereenkomst. Als u van plan bent om dit te doen, laat de kwestie dan vooraf toetsen door een advocaat.

Mag ik de sollicitant vragen mee te werken aan een aanstellingskeuring?
Op aanstellingskeuringen is de Wet op de medische keuringen van toepassing. Een aanstellingskeuring mag alleen worden uitgevoerd voor functies waarvoor bijzondere eisen op het punt van medische geschiktheid gelden. De bijzondere eisen moeten schriftelijk zijn vastgelegd. In de vacature moet staan dat een medische keuring voor de functie van belang is. De werkgever dient de gecertificeerde bedrijfsarts of arbodienst om advies te vragen alvorens de eisen op papier te zetten. Dit geldt ook ten aanzien van het doel van de keuring, de vragen die over de gezondheid zullen worden gesteld en de vraag welke medische onderzoeken mogen worden verricht. Deze adviesaanvraag geschiedt schriftelijk. Daarnaast mag een sollicitant pas worden gevraagd hieraan mee te werken als de werkgever van plan is hem aan te nemen. Meestal dus aan het einde van het sollicitatieproces.

Hoe lang mag een sollicitatiebrief, curriculum vitae en de gespreksaantekeningen bewaard worden?
Tot uiterlijk vier weken nadat de sollicitatieprocedure is beëindigd. Met toestemming van de sollicitant mag de termijn worden verlengd met een jaar, bijvoorbeeld omdat er binnenkort mogelijk een andere passende functie beschikbaar komt. Als de sollicitant in dienst treedt, mogelijk de gegevens bewaard blijven tot 2 jaar na het einde van de arbeidsovereenkomst.

Mag ik internet raadplegen om aan informatie over de sollicitant te komen?
Ja, dat mag. Het advies is wel hier terughoudend mee om te gaan, temeer aangezien niet alle informatie op internet juist is en u meer informatie kunt aantreffen dan noodzakelijk is om de geschiktheid van een sollicitant voor de functie te kunnen beoordelen. U moet altijd nagaan of er andere, minder verstrekkende mogelijkheden zijn om aan informatie te komen. Zo kunt u de sollicitant vragen stellen (niet over bijv. gezondheid of zwangerschap/kinderwens) of een referentiecheck doen met zijn toestemming. Bovendien moet u als werkgever vooraf aan de sollicitant laten weten dat u informatie over de sollicitant gaat zoeken op het internet en deze wordt betrokken in het sollicitatietraject. Als u de gegevens van het internet betrekt bij de sollicitatieprocedure moet u de sollicitant de mogelijkheid bieden om een reactie te kunnen geven op deze gevonden informatie.

Mag ik informatie inwinnen bij de voormalig werkgevers van de sollicitant?
Ja, dat mag met vooraf van de sollicitant verkregen toestemming (bij voorkeur schriftelijk), tenzij deze toestemming op grond van de wet of nadere regelgeving niet is vereist De te verkrijgen informatie moet wel direct verband houden met de te vervullen vacature. Als dit onderdeel is van uw aannamebeleid, moet u rekening houden met instemmingsrecht van de ondernemingsraad.

Mag ik referenties natrekken?
Ja, als u vooraf toestemming van de sollicitant heeft gekregen, tenzij deze toestemming op grond van de wet of nadere regelgeving niet vereist is De te verkrijgen informatie moet wel direct verband houden met de te vervullen vacature.

Wij willen een regeling invoeren met betrekking tot screening van sollicitanten, wie betrekken wij daarbij?
Voor de invoering, wijziging of intrekking van dit soort beleid heeft u voorafgaande instemming van de ondernemingsraad of personeelsvertegenwoordiging nodig op grond van de Wet op de Ondernemingsraden.

Wat betekent de identificatieplicht voor de werkgever?
De identificatieplicht voor de werkgever bestaat uit drie onderdelen:
1. de verificatieplicht betekent dat u het identiteitsbewijs van werknemers bij indiensttreding moet controleren op echtheid en geldigheid
2. de bewaarplicht houdt in dat u zelf een kopie maakt van het identiteitsbewijs van alle werknemers die u in dienst neemt en deze in uw administratie bewaart. Als de geldigheid van het identiteitsbewijs gedurende het dienstverband verloopt, hoeft u niet opnieuw een kopie te maken.
3. de zorgplicht betekent dat u uw werknemers bij controle in de gelegenheid moet stellen aan hun identificatieplicht te voldoen. U moet uw werknemers erop wijzen dat zij ook tijdens het werk een geldig identiteitsbewijs bij zich moeten dragen. Dit geldt voor mensen die rechtstreeks bij u in dienst zijn, en ook voor inleenkrachten.

Wat is een geldig identiteitsbewijs?
Dit kan bijvoorbeeld een paspoort zijn, een identiteitskaart of vreemdelingendocument. Het mag géén rijbewijs zijn. Op het rijbewijs staat namelijk niets over de nationaliteit en verblijfstatus.
De werknemer is verplicht het originele document te tonen. Bij het controleren van identiteitsbewijzen moet gelet worden op:

- de pasfoto: komt deze overeen met de persoon die voor u staat?
- kenmerken: kloppen de genoemde fysieke kenmerken zoals lengte en leeftijd?
- handtekening: laat de medewerker ter controle zichtbaar een handtekening zetten
- nationaliteit: de identificatieplicht geldt ook voor buitenlandse werknemers

- geldigheid van het document: is de vervaldatum nog niet verstreken?

Hoe lang moet ik een kopie van het identificatiebewijs bewaren?
De bewaartermijn is tot vijf jaar na het einde van het dienstverband.

Als de geldigheid van het identificatiebewijs gedurende het dienstverband is verstreken moet het dan ververst worden?
Nee, als de geldigheid van het identiteitsbewijs gedurende het dienstverband verloopt, hoeft het niet ververst te worden. Het gaat om het identiteitsbewijs op het moment van indiensttreding.
Geldt de identificatieplicht ook voor uitzendkrachten?
Als u een uitzendkracht inhuurt via een uitzendbureau, moet u ook als inlenende werkgever zelf het originele identiteitsbewijs van de uitzendkracht controleren. U doet dit voor aanvang van de werkzaamheden. U hoeft geen kopie van het identiteitsbewijs in uw administratie op te slaan.

Hoe kun je gegevens van kandidaten verzamelen?
Gegevens kunnen op directe en op indirecte wijze worden verzameld. Bij de directe wijze geeft de kandidaat rechtstreeks gegevens door, bijvoorbeeld via een sollicitatieformulier. Bij de indirecte wijze worden de gegevens via een externe bron verzameld. Dit gebeurt bijvoorbeeld als HR gegevens over de kandidaat uit LinkedIn haalt

Wat zijn de eisen als je gegevens direct van de kandidaat ontvangt?
Als de gegevens direct van de kandidaat komen, dan dient het privacy statement te worden verstrekt op het moment dat de persoonsgegevens doorgegeven worden. Dit kan door een link naar het privacy statement op te nemen op het sollicitatieformulier.

Mag je persoonsgegevens vanuit LinkedIn opslaan?
Wanneer gegevens op indirecte wijze worden verzameld, bijvoorbeeld via LinkedIn, gelden dezelfde eisen als voor directe wijze zijn aangegeven. Daarnaast moet je duidelijk aangeven welk soort (categorie) gegevens je hebt verwerkt en welke bron je hiervoor gebruikte.
De betrokkene dient binnen een redelijke termijn (in ieder geval binnen een maand na verwerking) geïnformeerd te worden over bovenstaande punten. Als de persoonsgegevens verwerkt worden om te communiceren met de betrokkene, dan dient deze informatie op zijn laatst tijdens het eerste contact met de betrokkene verstrekt te worden.

Hoe ga je om met telefonische toestemming van een kandidaat?
Telefonische toestemming is volgens de wet ook een indirecte verzameling (zoals LinkedIn) er dient na het telefoon gesprek een privacy verklaring uitgestuurd te worden waar de persoon akkoord op kan geven als documentatie/registratie.

Iemand laat zijn gegevens achter op Linkedin. Mag ik die persoon contacteren en de informatie opslaan om een functie voor te stellen?
Je mag diegene benaderen. Hij/zij heeft zelf de gegevens online gezet. Om ze in je eigen database te bewaren zul je toestemming moeten vragen. Dat kan door je vraag te stellen en te vragen om toestemming te gegeven om gegevens te bewaren.

Hoe lang mag ik kandidaat-gegevens bewaren?
We kunnen een vijftal fasen onderkennen in het proces met mogelijk een andere grondslag voor het bewaren van de persoonlijke gegevens en met verschillende bewaartermijn. Deze stel je vast in je eigen privacy statement.

Hoe lang mag je gegevens bewaren van 1ste fase: Zoeken en vinden van potentiële kandidaten
Omdat er nog geen contact is met de kandidaat heb je nog geen toestemming kunnen verkrijgen. Om de kandidaat te kunnen benaderen zul je toch de bijvoorbeeld via social media, websites of aangekochte bestanden gevonden gegevens moeten kunnen gebruiken (check op AGV compliant van die partijen). En als je dit passend bij je focus profielen en niet in bulk doet, kan je een gerechtvaardigd belang aanvoeren.om toch deze gegevens tijdelijk op te slaan (bijvoorbeeld 4 weken).Deze belangenafweging tussen het belang van de recruitment en het individuele belang zul je in je verwerkingsregister moeten onderbouwen en documenteren.

Hoe lang mag je gegevens bewaren van 2de fase: Contact opnemen met potentiële kandidaten
Op het moment van contact kan toestemming gevraagd worden om de kandidaat te benaderen voor relevante vacatures. Dit kan via een duidelijke opt-in button. Tijdens dit proces van toestemming vragen kun je de gegevens 30 dagen in je database bewaren.
Als je toestemming hebt verkregen kun je de persoonsgegevens in overeenstemming met de eigen policy statement de aangegeven termijn bewaard worden (richtlijn 12 maanden). En vervolgens contact opnemen over de afgesproken onderwerpen (nieuwsbrief, openstaande vacatures, gerichte vacatures, etc).

Hoe lang mag je gegevens bewaren van 3de fase: Voorstellen van kandidaten / sollicitatie?
Informatie die je verzameld over de persoon, relevant voor het welslagen van de vacature-invulling, zal je nadat duidelijks dat degene niet wordt voorgesteld, verwijderd moeten worden. Wil je de gegevens toch bewaren, zul je hiervoor apart toestemming moeten vragen.
Dit geldt ook voor het delen van persoonsgegevens met potentiële opdrachtgevers. In je policy statement heb je vastgelegd hoe lang potentiële opdrachtgevers de persoonsgegevens mogen bewaren. Bijvoorbeeld 2 weken nadat een persoon is afgewezen alle gegevens door opdrachtgever te verwijderen. Er is namelijk geen grondslag om de gegevens langere bewaren. Als een opdrachtgever andere termijnen hanteert dan in je policy statement staat, zul je dit apart dienen te vermelden.
Eigen bewaartermijn Sollicitatiegegevens: 1 jaar met toestemming, of afwijkende termijn als onderbouwd is in policy statement.

Hoe lang mag je gegevens bewaren van 4de fase: Aanstelling?

- Na de aanstelling zullen een aantal gegevens wettelijk bewaard moeten worden.
- Salarisadministratie voor fiscus: 7 jaar bewaarplicht.
- Kopie identiteitsbewijs: 5 jaar na einde dienstverband
- Verklaring Loonbelasting: 5 jaar na einde dienstverband
- Personeelsfile: richtlijn 2 jaar (als onderbouwd kan worden)

Hoe lang mag je gegevens bewaren van 5de fase: Contact houden na afwijzing voor mogelijke andere aanstelling?
Na de afwijzing kun je toestemming vragen om in database te houden voor andere doeleinden dan wettelijke vereisten. Dit is vergelijkbaar met fase 3. In recent uitgebrachte beleidsadvies van een adviesorgaan van de Europese Commissie (de Working Party 29, waarin de nationale toezichthouders vertegenwoordigd zijn) wordt aangegeven dat persoonsgegevens, die tijdens het recruitmentproces worden verzameld, in het algemeen verwijderd dienen te worden op het moment dat duidelijk is dat de kandidaat niet aangenomen wordt.
Wil je de gegevens van de kandidaat behouden voor eventuele toekomstige vacatures en aanbiedingen, dan moet je de kandidaat hierover te informeren en toestemming vragen. Hij moet hierbij de mogelijkheid krijgen om hiertegen bezwaar te maken, waarna hij alsnog verwijderd dient te worden.

HR. SROI

Wat zegt de Autoriteit Persoonsgegevens over SROI?

Hoe vragen overheden aan opdrachtnemers met een contractuele social return verplichting deze aan te tonen?

- Wat de inzet voor social return is geweest.
- Dat de ingezette werknemers in het kader van social return daadwerkelijk horen tot een doelgroep uit het bouwblokkenmodel zoals opgenomen in het uitvoeringsprotocol.

Om welke werkgeversgegevens gaat het?

- NAW-gegevens
- Geboortedatum
- Bewijs van uitkering/ doelgroepenverklaring (P-wet, Wajong, WW, WAO/ WIA, WSW, VSO, PrO)
- Arbeidsovereenkomst/ stageovereenkomst

Waarvoor zijn de SROI gegevens nodig?

- De NAW-gegevens en geboortedatum zijn noodzakelijk om te kunnen vaststellen dat het om een uniek persoon gaat. Daarmee controleert een gemeente ook of een persoon niet meerdere keren wordt opgevoerd.
- Met het bewijs van uitkering/ doelgroepenverklaring wordt vastgesteld dat de werknemer tot de doelgroep met een afstand tot de arbeidsmarkt behoort.
- Met de arbeidsovereenkomst/ stageovereenkomst wordt vastgesteld dat de werknemer daadwerkelijk in dienst is bij de werkgever. Met de begin- en einddatum van de overeenkomst wordt bepaald hoe lang iemand (naar rato) kan meetellen voor de social return invulling.

Waarom worden persoonsgegevens uitgewisseld en mag dat ook?
Om verantwoording af te kunnen leggen ten aanzien van de contractuele SROI-verplichtingen moeten bewijsstukken overlegd worden waaruit blijkt dat een kandidaat tot de doelgroep Social Return behoort. De grondslag voor het verstrekken van die gevraagde gegevens aan een gemeente is “gerechtvaardigd belang”.
Het is een gemeente op grond van de Aanbestedingswet toegestaan om bij aanbestedingen bijzondere voorwaarden toe te passen die verband houden met sociale overwegingen. Om te kunnen controleren of de werkgever zich aan de contractuele afspraken houdt die in het kader van de aanbesteding gemaakt zijn, in dit geval betreffende social return, mogen persoonsgegevens worden verwerkt op basis van de grondslag “nakomen van een wettelijke verplichting”.
In het verleden is voorgekomen dat een werknemer meerdere keren werd opgevoerd, niet tot de doelgroep behoorde of niet naar rato werd opgevoerd op een opdracht van de gemeente. In het belang van het via social return bieden van kansen aan mensen met een afstand tot de arbeidsmarkt, is het daarom noodzakelijk dat persoonsgegevens worden verwerkt en gecontroleerd voor het nakomen van de social return contracteis van werkgever/opdrachtnemer.

Wat is WIZZR?
WIZZR is een web-based systeem waarin bijgehouden wordt in hoeverre een opdrachtnemer aan zijn SROI-verplichting heeft voldaan. Zo'n 70 overheden (gemeenten, provincies, waterschappen) en zo'n 1800 opdrachtnemers maken gebruik van WIZZR.
Het systeem is ontwikkeld door een aantal ondernemers die op zoek waren naar een systeem waarmee ze hun social return verplichtingen op een eenvoudige manier inzichtelijk konden maken. Belangrijk uitgangspunt van de ontwikkelaars is dat SROI iets is dat je samen doet en dat je een gebruiksvriendelijk systeem nodig hebt dat proces ondersteunend is.

Wie is verantwoordelijk voor invoeren gegevens in WIZZR?
De verantwoordelijkheid voor de invulling van de social return verplichting en het aanleveren van gevraagde gegevens en bewijsstukken in het registratiesysteem WIZZR, ligt volledig bij opdrachtnemer zelf. Het niet voldoen aan de verplichting kan resulteren in het terug moeten betalen van het openstaande bedrag.

Hoe weet WIZZR wat ik aan SROI kan opvoeren op het project dat ik onderhanden heb?
De SROI paragraaf uit het bestek staat in WIZZR. Daar zorgt de opdrachtgever voor. De opdrachtnemer voert in het systeem in wat hij aan SROI heeft gedaan en vinkt aan wat voor soort activiteit het is. Als de opdrachtgever de bijdrage van de opdrachtnemer accepteert, wordt de bijdrage verwerkt in het systeem.

Wie kunnen er in WIZZR kijken?
De partijen die betrokken zijn bij het contract kunnen de gegevens zien die bij dat contract horen. Deze partijen worden geautoriseerd door de opdrachtgever. Alleen de gegevens die door de opdrachtgever zijn goedgekeurd, zijn zichtbaar.

Hoe lang worden de persoonsgegevens in WIZZR bewaard?
Dat bepaalt de opdrachtgever. Overheden hanteren meestal de richtlijnen van de Archiefwet. Het staat de opdrachtnemer echter vrij om, als het project is afgerond, persoonsgegevens te verwijderen.

83. HR. Spionagesoftware medewerkers

Wat zegt de Autoriteit Persoonsgegevens over spionagesoftware ?

- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-uitkering/controle-van-personeel
- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-uitkering/controle-van-personeel#welke-voorwaarden-gelden-voor-de-heimelijke-controle-van-werknemers-4621

Wat zeggen andere over spionagesoftware?
https://www.ploum.nl/vakantie-in-de-baas-zijn-tijd-houd-het-gebruik-van-gluursoftware-binnen-de-perken/

Massaal thuiswerken, massaal meegluren?
Bij pandemie is een van de belangrijkste veranderingen het massaal thuiswerken. Werkgevers schaffen massaal 'spionagesoftware' aan, om hun werknemers thuis te kunnen volgen. Controle van werknemers is in principe niet verboden, maar er gelden wel strikte voorwaarden en de mogelijkheden zijn dan ook begrensd. Heimelijk gluren is veelal niet toegestaan. Met het monitoren van werknemers is veelal sprake van verwerking van persoonsgegevens. Hierop zijn de Algemene Verordening Gegevensbescherming (AVG) en gerelateerde privacywetgeving van toepassing. Voorts is art. 7:611 BW van belang: werkgever en werknemer zullen zich als goed werkgever respectievelijk werknemer dienen te gedragen. Daarbij hoort dat de werkgever de persoonlijke levenssfeer van de werknemer respecteert.
Welke mogelijkheden van en voorwaarden voor controle van thuiswerkende werknemers? We laten daarbij de (arbeidsrechtelijke) vraag wat er eventueel met de uitkomst zou kunnen worden gedaan daarbij even buiten beschouwing.

Gerechtvaardigd belang werkgever?
De werkgever moet een gerechtvaardigd belang hebben (lees: een legitieme reden) om werknemers te controleren middels een personeelsvolgsysteem. Dit belang moet zwaarder wegen dan het privacybelang van haar werknemers. Een van de belangrijkste vragen die daarbij moet worden gesteld is: is het op deze wijze monitoren van werknemers noodzakelijk? Zijn er andere, minder ingrijpende manieren om het betreffende doel te bereiken? Dit dient van geval tot geval te worden beoordeeld en kan nog wel eens tot een negatieve uitkomst leiden in dit kader. Zo zal in de regel wellicht kunnen worden volstaan met het (eerst) 'anoniem' monitoren van computergebruik. Een werkgever zal eerder een gerechtvaardigd belang kunnen hebben, indien er sterke aanwijzingen zijn dat een thuiswerkende werknemer zonder goede reden zijn of haar werk niet uitvoert. Een vervolgvraag kan dan zijn of het dan niet meer zin heeft om de werknemer om opheldering te vragen in een gesprek, of dat (heimelijke) controle in dit geval toch nodig is. Vertrouwen staat altijd voorop. Het is ook belangrijk in acht te nemen dat inmiddels wel aanvaard is dat werknemers ook tijdens werktijd enige tijd aan privézaken moeten kunnen besteden. Even 'Facebooken'? Moet kunnen, indien met mate. Bovendien zijn er ook geluiden dat meer pauze tijdens het thuiswerken en een kortere werkdag aanhouden juist belangrijk ofwel volstrekt normaal is.

Welke informatieplicht
Als deze toets is doorstaan, is het belangrijk werknemers te informeren over het feit dat controle plaatsvindt of kan plaatsvinden, maar ook over de regels waaraan de werknemer zich moet houden. In het kader van de AVG is het belangrijk de werknemer ook te informeren welke persoonsgegevens daarbij worden verwerkt, hoe lang deze worden bewaard, wat zijn/haar rechten zijn etc.

Dit kan bijvoorbeeld middels het personeelshandboek of een privacyverklaring voor werknemers, en is heel belangrijk in het kader van de rechtmatigheid van de controle. Heimelijke controle is – kort gezegd – alleen toegestaan als er een redelijke verdenking van bijvoorbeeld diefstal of fraude bestaat en mag slechts incidenteel zijn. In het algemeen is het voorafgaand aan de inzet van spionagesoftware verstrekken van duidelijke informatie over de (mogelijke) controle noodzakelijk is.

Welke beperking van de controle?
De controle dient zich te beperken tot wat noodzakelijk is voor het betreffende doel. Stel van tevoren als werkgever dus goed de grenzen vast en zorg ook dat slechts een beperkt aantal bevoegde personen de uit de controle verkregen gegevens kunnen inzien. Een werkgever dient zich ook te onthouden van het bekijken van berichten (bijvoorbeeld e-mail) die als privé zijn aangemerkt. Hoewel niet zaligmakend, kan het werknemers en werkgevers helpen als een werknemer in zijn/haar e-mailbox een mapje “Privé” aanmaakt. En hoe vaak is controle nu echt nodig voor het betreffende doel? H

Welke type software relevant?
Bij het doorlopen van voornoemde toets dient de werkgever in ogenschouw te nemen wat de betreffende software precies doet. Als alleen de schermtijd wordt gemeten zal de toets makkelijk worden doorstaan dan wanneer om de zoveel tijd screenshots worden gemaakt van de openstaande pagina’s. Daarmee bestaat ook een veel grotere kans dat (meer) persoonsgegevens worden verwerkt c.q. privéinformatie wordt verzameld. Het is sterk de vraag of dat niet een te vergaande inbreuk maakt op de privacy van werknemers. Het nieuwsbericht noemt ook het maken van foto’s van de werknemer, dat lijkt in ieder geval een brug te ver.

Welke afspraken met softwareleverancier?
Uiteraard moeten ook goede afspraken met de softwareleverancier worden gemaakt: veelal zal een verwerkersovereenkomst nodig zijn. Let ook op het privacy beleid van de leverancier en houd daarbij ook in het oog dat potentieel klantgegevens/ gevoelige gegevens ook worden verwerkt door de spionagesoftware te gebruiken. Het kan dan ook zijn dat uw externe privacy beleid ook moet worden aangescherpt.

Is toestemming vragen een mogelijke oplossing?
Kan een werkgever niet gewoon om toestemming vragen in deze crisistijd? Nee, om gegevens te verwerken op grond van toestemming moet deze vrijelijk worden gegeven. Kort gezegd wordt aangenomen dat van ‘vrijelijke toestemming’ in een arbeidsrelatie geen sprake kan zijn.

Is een DPIA en instemming OR vereist?
Afhankelijk van de mate van controle zal een Data Protection Impact Assessment (DPIA) moeten worden verricht, voordat de werkgever de software mag inzetten. Dat is ook relevant voor de verantwoordingsplicht onder de AVG; in welk kader dan ok het advies om voornoemde toets te verslaan en het verslag te bewaren. Verder zal een ondernemer eerst instemming moeten vragen aan de Ondernemingsraad voordat de ondernemer ‘gluursoftware’ of een vergelijkbaar controlesysteem (personeelsvolgsysteem) introduceert, maar ook als er een thuiswerkprotocol wordt ingesteld of aangepast.

84. HR. Strafrechtelijke gegevens

Wat zegt de Autoriteit Persoonsgegevens over strafrechtelijke gegevens?
Zie: https://autoriteitpersoonsgegevens.nl/nl/melden/voorafgaand-onderzoek/strafrechtelijke-gegevens

Mag ik persoonsgegevens van strafrechtelijke aard verwerken?
Persoonsgegevens die betrekking hebben op strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen, alsmede persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag ('persoonsgegevens van strafrechtelijke aard'), mogen alleen worden verwerkt op basis van een gerechtvaardigde grondslag onder toezicht van de overheid en voor zover toegestaan in de Uitvoeringswet.

Wat zijn de algemene uitzonderingsgronden op het verbod om persoonsgegevens van strafrechtelijke aard te verwerken?
Het gaat om:

- de uitdrukkelijke toestemming van de betrokkene;
- situaties waar de verwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of
- een andere natuurlijke persoon (indien de betrokkene fysiek of juridisch niet in staat is toestemming te geven);
- situaties waar de verwerking heeft betrekking op gegevens die door de betrokkene openbaar zijn gemaakt;
- situaties waar de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een vordering;
- gerechten die handelen in het kader van hun rechtsbevoegdheid;
- situaties waar de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang;
- situaties waar de verwerking noodzakelijk is met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden en is voldaan aan alle toepasselijke voorwaarden uit de Verordening

Mag ik persoonsgegevens van strafrechtelijke aard verwerken bij een beoordeling?
U mag persoonsgegevens van strafrechtelijke aard verwerken wanneer dit nodig is voor de beoordeling van een verzoek van een betrokkene om een beslissing over hem te nemen of aan hem een
prestatie te leveren. Een voorbeeld is een screening in het kader van een sollicitatieprocedure voor een
integriteitsfunctie. Onder omstandigheden mogen voor een dergelijk doel persoonsgegevens van strafrechtelijke aard worden verwerkt.

Mag ik persoonsgegevens van strafrechtelijke aard verwerken ter bescherming van de eigen belangen, als strafbare feiten jegens MAAS zijn gepleegd of worden verwacht te zullen worden gepleegd?
Ja dat mag. Denk dan bijvoorbeeld aan camerabeelden waarop een diefstal te zien is. Dit zijn persoonsgegevens van strafrechtelijke aard, omdat er een strafbare handeling op te zien is die direct aan een persoon is te relateren. Deze persoonsgegevens mag u ten behoeve van uzelf wel verwerken in afwijking van de hoofdregel, maar mag u niet zonder meer openbaar maken. Nota Bene:
Het is alleen toegestaan om persoonsgegevens van strafrechtelijke aard over uw medewerkers te verwerken, indien dit geschiedt overeenkomstig regels die zijn vastgesteld in overeenstemming met de
procedure bedoeld in de Wet op de ondernemingsraden.

Mag ik persoonsgegevens van strafrechtelijke aard ten behoeve van een derde (bijvoorbeeld een ander bedrijf) verwerken?
Dit is alleen toegestaan in de volgende gevallen:

- u heeft een vergunning op grond van de Wet op de particuliere beveiligingsorganisaties en recherchebureaus; of
- u verwerkt rechtmatig gegevens van medewerkers ten behoeve van een groepsmaatschappij (bijvoorbeeld een dochterorganisatie); of
- indien de verwerking noodzakelijk is met het oog op een zwaarwegend algemeen belang van een derde, passende waarborgen zijn getroffen ter bescherming van de persoonlijke levenssfeer van de betrokkene én de Autoriteit Persoonsgegevens u een vergunning heeft verleend voor de verwerking.

85. HR. Verklaring van Geen Bezwaar (VGB)

Wat zegt de rijksoverheid over VGB:
https://www.rijksoverheid.nl/onderwerpen/arbeidsovereenkomst-en-cao/vraag-en-antwoord/wanneer-vindt-er-een-veiligheidsonderzoek-plaats

Valt een VGB-document onder de AVG?
Nee, maar wel onder eigen (privacy) wetgeving. Wie een vertrouwensfunctie gaat vervullen, heeft een 'verklaring van geen bezwaar' (VGB) nodig. Hiervoor voert de AIVD een veiligheidsonderzoek uit. Net als iedereen is de AIVD gebonden aan wet- en regelgeving. Het werk van de dienst ligt verankerd in de Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017) en Wet op de Veiligheidsonderzoeken (Wvo) als het gaat om het verrichten van veiligheidsonderzoeken. Bij het tot stand komen van de Wiv vormde de privacy van burgers een belangrijk uitgangspunt. De Wiv 2017 is gebaseerd op de voorwaarden uit het Europees Verdrag tot bescherming van de rechten van de mens (EVRM), de jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) en de Grondwet.

Mag een VGB gecommuniceerd worden?
Dat mag je communiceren met de betreffende klant, met als wettelijke grondslag in ieder geval het uitvoeren van een overeenkomst. De klant is voor deze persoonsgegevens zelfstandig Verwerkingsverantwoordelijke.

Moet de VGB-verwerking opgenomen worden in het MAAS verwerkingsregister.
Ja, anders kan er geen veiligheidsonderzoek worden ingesteld en betrokkene mag wettelijk gezien niet op de betreffende vertrouwensfunctie zitten.
https://www.avgregisterrijksoverheid.nl/Ministerie_van_EZK_en_Ministerie_van_LNV/150_Veiligheidsonderzoeken_vertrouwensfuncties.html

86. HR. Verklaring Omtrent Gedrag (VOG)

Wat zegt de Autoriteit Persoonsgegevens over de VOG?
De Wet justitiële en strafvorderlijke gegevens (Wjsg) regelt het verwerken van justitiële gegevens (in persoonsdossiers) en de Verklaring Omtrent het Gedrag (VOG). De wet regelt ook de verwerking van strafvorderlijke gegevens.
De Autoriteit verwijst door naar: https://www.justis.nl/producten/vog/

Aanvullende bron: https://www.awvn.nl/privacy-arbeidsrelatie-sollicitatie/

Kan ik een medewerker verplichten een VOG aan te vragen en te verstrekken?
Ja, een werkgever kan een (toekomstig) werknemer verplichten een Verklaring omtrent gedrag (VOG) aan te vragen bij de gemeente waar hij staat ingeschreven en deze aan de werkgever te geven. Dit is relevant bij werkzaamheden waarbij kwetsbare personen of vertrouwelijke gegevens in het spel zijn. Voor sommige beroepen is een VOG zelfs verplicht, zoals voor leraren en taxichauffeurs.

Hoe een VOG aan te vragen?
Een VOG kunt u op twee manieren aanvragen: via de gemeente of via Justis.
De meest voorkomende weg is digitaal via de website van de dienst Justis van het ministerie van Veiligheid en Justitie. Daarnaast kan er een formulier worden afgehaald bij de gemeente. De werkgever moet op het formulier aangeven wat het doel van de aanvraag is en moet de aanvraag ondertekenen. Als dit niet is gebeurd wordt de aanvraag niet in behandeling genomen. De aanvrager zelf levert het aanvraagformulier in bij de afdeling burgerzaken van de gemeente waar deze staat ingeschreven.
Binnen 2 tot maximaal 4 weken na ontvangst van de aanvraag wordt de beslissing genomen. Dit is anders als er door de aanvragen strafbare feiten zijn gepleegd. Een beslissing vindt dan plaats binnen 8 weken na ontvangst van de aanvraag. De VOG wordt naar het huisadres van de aanvrager gestuurd.
Wanneer wordt de VOG niet afgegeven?
Als de aanvrager van de VOG in aanraking is geweest met justitie, wordt beoordeeld of de strafbare feiten een belemmering (kunnen) vormen voor de afgifte van een VOG. Voordat een VOG definitief wordt geweigerd, ontvangt de aanvrager eerst een voornemen tot afwijzing. Hierin staan de redenen van de voorgenomen afwijzing. De aanvrager kan schriftelijk aangeven waarom hij vindt dat hij wel een VOG zou moeten krijgen. Als het negatieve oordeel definitief is, ontvangt de aanvragen een afwijzende beschikking VOG, daartegen kan binnen zes weken bezwaar gemaakt worden.

Wat is de geldigheidsduur van een VOG?
De VOG heeft geen vaste geldigheidsduur. Vaak is de verklaring onbeperkt geldig voor het doel van de aanvraag. Het is ook mogelijk dat de werkgever om de zoveel jaar om een nieuwe VOG vraagt. De werkgever bepaalt hoe recent de VOG moet zijn.

Heb ik voldoende aan een fotokopie van een VOG?
Het is niet verboden een fotokopie van een VOG te maken. Als de medewerker het origineel wil behouden, dan kunt u het beste zelf een fotokopie van het origineel maken. Dit om te controleren of de medewerker in het bezit is van een echte VOG. De werkgever mag ook verlangen dat de originele VOG wordt ingeleverd.

Mag de originele VOG van een MAAS medewerker naar een klant gestuurd worden?

Ja, klant kan dit vereisen en de persoonsgegevens worden dan door klant beschermd, een en ander conform EU richtlijn 2016/680 en de implementerende wetten daarvan voor Nederland.
Voor alle nieuwe MAAS medewerkers is een “Verklaring Omtrent het Gedrag” (VOG) verplicht. Deze zal dan in het Personeelsdossier gearchiveerd worden. Indien een originele VOG van de MAAS medewerker naar de klant gaat, dan heeft MAAS geen verplichting om de originele VOG te bewaren, MAAS kan volstaan met een afschrift (digitaal) te bewaren. Advies om die kopie te voorzien van datum, handtekening en de tekst "origineel gezien, c.q. origineel naar klant xxx".

Mag een operator diens VOG inleveren bij de klant?
Ja, klant kan dit zelfs vereisen en de persoonsgegevens dan beschermd door klant, een en ander conform EU richtlijn 2016/680 en de implementerende wetten daarvan voor Nederland.

Waarom vraagt MAAS naar een VOG?
In alle functies waarin medewerkers aan de slag gaan met kwetsbare mensen, vertrouwelijke gegevens, geld of kostbare goederen, is een medewerker verplicht om een VOG aan te vragen. Justis kijkt of de (beoogde) medewerker strafbare feiten op zijn naam heeft. Als dat zo is dan kijkt Justis hoe groot de kans is op herhaling en of herhaling een risico voor de samenleving oplevert binnen de beoogde functie. Elke VOG-aanvraag is dus maatwerk. Een VOG geeft MAAS een stukje extra zekerheid van betrouwbaar personeel. Volledige zekerheid geeft een VOG niet: De delicten op een strafblad tellen na vier jaar niet meer mee bij een aanvraag voor de VOG.

Wordt een VOG versterkt als je een strafblad hebt?
Voor veel functies is er tegenwoordig een screeningsprocedure waarin een medewerker een Verklaring Omtrent Gedrag (VOG) moet overleggen. Je kunt ook een VOG krijgen als je een strafblad hebt. Dat komt omdat er geen belangrijke relatie tussen het vergrijp en de te vervullen functie werd geconstateerd. In dat geval krijg je dus gewoon een VOG: je persoonlijke belang om een inkomen te kunnen vergaren is groot en daarom moet er een relatie zijn tussen het weigeren van een VOG en de te vervullen functie (en zelfs dan moet het vergrijp vallen binnen een bepaalde terugkijktermijn).

Hoe controleert MAAS een VOG?
De controleprocedure moet aan een paar punten voldoen. Meestal wordt een VOG gescand en naar het belanghebbende bedrijf gemaild. Dit is echter niet de juiste procedure. De juiste procedure conform AVG is: De originele, geldige VOG moet worden gecontroleerd op echtheid. Die echtheidskenmerken kun je niet controleren aan de hand van een scan of kopie. Een dergelijke controle heeft geen rechtsgeldigheid. Het komt er dus op neer dat je een VOG in persoon moet laten zien.
Om de procedure netjes af te ronden, schrijf je op de VOG “origineel gezien, datum en naam medewerker of bedrijf”. Vervolgens leg je in een registratiesysteem vast wie het origineel heeft gecontroleerd, op welke datum en of de medewerker met de VOG voldoet aan de eisen. Dat kan bijvoorbeeld op schrift, dan kun je ook de handtekening van de controleur en de medewerker vastleggen.

Mag ik een kopie van de VOG bewaren?
De originele VOG blijft van degene om wie het gaat. Het is niet nodig en zelfs af te raden een scan of kopie te maken voor dossiervorming, omdat je volgens de AVG moet aantonen dat die (gevoelige) gegevens nodig zijn. Dat is echter niet het geval; een registratiesysteem voldoet immers prima. Maak je toch een scan of kopie, doe dat dan nadat je op de VOG de controle (origineel gezien, datum, naam) hebt aangegeven. Je hebt er anders niks aan, want die kopie voorziet niet in de echtheidskenmerken (en die kopie geeft dus geen meerwaarde naast schriftelijke registratie van de controle).

Twijfelt je of een VOG echt is?
Neem dan contact op met Justis: https://www.justis.nl/contact/index.aspx

Mag ik een kopie van de VOG mailen?
Nee. In verband met privacy-issues is het sowieso onverstandig de VOG te mailen. Persoonlijke, gevoelige gegevens (zoals naam, adresgegevens, geboortedatum) komen dan in mailsystemen waar ze niet horen. Je hebt er geen controle meer over: wie heeft het document in de inbox, aan wie is het doorgestuurd, wanneer wordt het verwijderd? Vaak bestaan hier binnen organisaties ook geen procedures voor, terwijl dat volgens de AVG wel zou moeten. Merk op dat de overheid de VOG ook nooit digitaal toestuurt. Hoe je hem ook aanvraagt, hij wordt altijd per post toegestuurd, en uitsluitend geadresseerd aan de persoon om wie het gaat.

Hoe ga je als (beoogd) medewerker ermee om als je geen VOG krijgt?
Indien je VOG wordt geweigerd, dan krijg je eerst een zogenaamd voornemen tot weigeren toegestuurd. Hierin staan de redenen van de voorgenomen weigering van je VOG. Je kunt op dat moment schriftelijk je eigen zienswijze indienen en aanvullende informatie geven. Wanneer de weigering van je VOG definitief is, ontvang je een afwijzend besluit. Hiertegen kun je wel bezwaar maken. Mocht je bezwaar worden afgewezen, dan heb je nog de mogelijkheid om bij de bestuursrechter in beroep te gaan. Alle justitiële gegevens, dus ook openstaande zaken, mogen tegen iemand worden gebruikt bij het beoordelen van een Verklaring Omtrent het Gedrag-aanvraag. Concreet is er trouwens maar een kleine kans dus dat een persoon er een misloopt: In 2016 waren er in totaal 968.300 VOG aanvragen waarvan er 146.800 werden afgegeven terwijl de aanvrager veroordeeld is en werden er 3.650 afgewezen. Dit is maar 0,38% van het totaal aantal aanvragen.

Mag ik als werkgever een VOG van een werknemer doorsturen aan een opdrachtgever?
Dat mag alleen onder strikte voorwaarden. Maar meestal is het niet nodig dat u de verklaring omtrent het gedrag (VOG) doorstuurt aan de opdrachtgever als u een medewerker wilt uitlenen. Het is voldoende als u laat weten dat er geen belemmeringen zijn voor uw werknemer om bij de opdrachtgever aan de slag te gaan.

Vindt de opdrachtgever het noodzakelijk om te weten of er een VOG is afgegeven voor uw medewerker?
Of vindt u het zelf noodzakelijk om deze informatie met de opdrachtgever te delen? Dan moeten de opdrachtgever en u de noodzaak voor het uitwisselen van deze informatie kunnen motiveren. Het feit alleen dat de opdrachtgever de informatie opvraagt, is in dit geval niet voldoende.
Als u tegen de opdrachtgever zegt dat uw medewerker geen VOG heeft gekregen, is daaruit op te maken dat de medewerker een strafrechtelijk verleden heeft. U wisselt dan dus strafrechtelijke gegevens uit. Dit zijn zogeheten bijzondere persoonsgegevens, die organisaties alleen bij uitzondering mogen verwerken. Wilt u dergelijke informatie uitwisselen, dan moet u uw gegevensverwerking melden bij de Autoriteit Persoonsgegevens en hierbij een voorafgaand onderzoek aanvragen. Alléén wanneer de Autoriteit Persoonsgegevens een goedkeurende verklaring afgeeft voor uw verwerking, kunt u de opdrachtgever laten weten of uw werknemer een VOG heeft ontvangen.

87. HR. Verzuim

Wat mag werkgever wel vragen en registreren?
Een werkgever mag bij ziekmelding van de werknemer de volgende gegevens over gezondheid van de zieke werknemer vragen en registreren:

- het telefoonnummer en (verpleeg)adres; – de vermoedelijke duur van het verzuim;
- de lopende afspraken en werkzaamheden;
- of de werknemer onder een van de zogenaamde 'vangnetbepalingen' van de Ziektewet valt (maar niet onder welke vangnetbepaling hij valt);
- of de ziekte verband houdt met een arbeidsongeval;
- of er sprake is van een verkeersongeval waarbij een eventueel aansprakelijke derde betrokken is (regresmogelijkheid).

Ook mag een werkgever bijhouden hoe vaak een werknemer ziek is. De werkgever mag bij ziekmelding door de werknemer deze ziekmelding registeren, omdat deze registratie noodzakelijk is in het kader van de vaststelling van de loondoorbetalingsverplichting.

Wat mag werkgever niet vragen?
In dat kader mag de werkgever (en of functionarissen zoals casemanagers) de werknemer niet vragen naar een diagnose of behandeling door een arts, ook niet naar de functionele mogelijkheden en beperkingen van de werknemer. Dan gaat het om vragen als: 'hoeveel kun je nog tillen', 'kun je op je knieën zitten', 'hoe lang kun je geconcentreerd werken', 'is hectiek op de afdeling een probleem', 'kun je in een groep werken'. De werkgever mag de volgende gegevens niet vragen en/of vastleggen:

- (spontaan vertelde) oorzaak van het verzuim;
- eigen waarnemingen over de gezondheidstoestand van de werknemer;
- informatie over therapieën;
- afspraken met artsen, therapeuten of begeleiders;
- problemen uit het verleden of uit de privésfeer.

Wat kan werknemer zelf aangeven?
Van werknemer wordt verwacht dat deze indien mogelijk zélf aangeeft hoe lang deze niet in staat zal zijn de normale werkzaamheden uit te voeren en welke (deel) taken, (deel)functies of werkzaamheden deze zou kunnen verrichten.

Wat mag werkgever verwerken?
De werkgever mag de gegevens die de bedrijfsarts/arbodienst aan hem heeft verstrekt verwerken. Denk daarbij aan:

- de werkzaamheden waartoe de werknemer niet meer of nog wel in staat is (functionele beperkingen, restmogelijkheden en implicaties voor het soort werk dat de werknemer nog kan doen);
- de verwachte duur van het verzuim;
- de mate waarin de werknemer arbeidsongeschikt is (gebaseerd op functionele beperkingen, restmogelijkheden en implicaties voor het soort werk dat de werknemer nog kan doen);
- eventuele adviezen over aanpassingen, werkvoorzieningen of interventies die de werkgever voor de re-integratie moet treffen.

De werkgever mag, met uitzondering van bovenstaande gegevens, in principe geen andere gegevens over de gezondheid van de werknemer in zijn eigen administratie registreren en/of doorgeven aan de bedrijfsarts/arbodienst, ook niet als deze gegevens vrijwillig door de werknemer zijn verstrekt.

Het noodzakelijkheidsvereiste geldt namelijk ook wanneer gegevens over de gezondheid vrijwillig aan de werkgever zijn verstrekt.

Wat valt onder medisch beroepsgeheim van de bedrijfsarts?
Alle mogelijke gegevens over de gezondheid van werknemers, die voor de werkgever niet noodzakelijk zijn voor de loondoorbetalingsverplichting, noch voor de re-integratie/verzuimbegeleiding, onder het medisch beroepsgeheim van de bedrijfsarts. Het betreft onder meer de volgende gegevens:

- diagnoses, naam ziekte, specifieke klachten of pijnaanduidingen;
- eigen subjectieve waarnemingen, zowel over geestelijke als lichamelijke gezondheidstoestand;
- gegevens over therapieën, afspraken met artsen, fysiotherapeuten, psychologen e.d.;
- overige situationele problemen, zoals relatieproblemen, problemen uit het verleden, verhuizing, overlijden partner, scheiding e.d.

88. HR. Zieke werknemer

Bron:
https://www.awvn.nl/privacy-zieke-werknemers/
https://www.vno-ncw.nl/sites/default/files/een_knellend_probleem.pdf

Mag ik gegevens over de gezondheid van een medewerker vermelden in zijn personeelsdossier of op een andere plek?
Nee, dit zijn bijzondere persoonsgegevens en die mag u niet vermelden, tenzij dit gebeurt op basis van een wettelijke bepaling of de medewerker hiervoor uitdrukkelijk zijn toestemming geeft. Ook een constatering van een leidinggevende dat de medewerker een lichamelijke handicap heeft, mag niet worden geregistreerd.

Kan ik vragen naar de aard en de oorzaak van de ziekte?
Nee, daar mag u niet informeren. Doet u dat wel, dan is de zieke medewerker niet verplicht hierop te antwoorden, omdat dit onder de bescherming van zijn persoonlijke levenssfeer valt.

Welke gegevens mag ik wel vragen en noteren over de arbeidsongeschiktheid van de zieke medewerker?
U mag de volgende informatie bij de ziekmelding aan de medewerker vragen:

- het telefoonnummer en (verpleeg)adres;
- de vermoedelijke duur van het verzuim;
- de lopende afspraken en werkzaamheden;
- of de werknemer onder een van de vangnetbepalingen van de Ziektewet valt (maar niet onder welke vangnetbepaling hij valt);
- of de ziekte verband houdt met een arbeidsongeval;
- of er sprake is van een verkeersongeval waarbij een eventueel aansprakelijke derde betrokken is (regresmogelijkheid).

Is de medewerker wel verplicht de aard en oorzaak van de ziekte aan de bedrijfsarts te melden?
Ja, de zieke medewerker is op grond van de wet verplicht deze informatie aan de bedrijfsarts te verstrekken, zodat deze kan vaststellen of de medewerker arbeidsongeschikt is en in welke mate en of hij passende arbeid kan verrichten.

Wat kan ik doen als de zieke medewerker de bedrijfsarts niet informeert over de aard en oorzaak van zijn ziekte en daarmee de ziekteverzuimvoorschriften niet naleeft?
U kunt het loon opschorten voor de tijd dat de zieke medewerker de bedrijfsarts daarover niet informeert en daarmee niet voldoet aan de controlevoorschriften zoals die gelden binnen uw organisatie. U kunt uw voorgenomen besluit tot loonopschorting het beste vooraf laten toetsen. U kunt hiervoor contact opnemen met de advocaten van AWVN.

Als ik gerede twijfel heb of de medewerker wel echt ziek is, kan ik dan een recherchebureau inschakelen?
Bij voorkeur niet. Terughoudendheid is geboden, omdat het recht op privacy van de medewerker daarmee in het geding komt. Bij een ernstige verdenking dat de medewerker zich schuldig maakt aan overtreding van de verzuimvoorschriften is een onderzoek denkbaar. Het verdient aanbeveling voor het instellen van een onderzoek de medewerker om opheldering te vragen. Als daarmee de verdenking blijft, is inschakeling van een recherchebureau denkbaar en moeten observaties zich beperken tot waarnemingen op de openbare weg. Na afloop moet het onderzoek ook gemeld

worden aan de medewerker. Voordat u een recherchebureau inschakelt, kunt u het beste een advocaat benaderen voor advies en begeleiding.

89. Identificatie. BSN nummer

Wat zegt de Autoriteit Persoonsgegevens over het Burgerservicenummer (BSN):
https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/identificatie/burgerservicenummer-bsn

Wat zegt UWV over het Burgerservicenummer (BSN):
Handleiding aanvraag ontslagvergunning wegens bedrijfseconomische redenen: geraadpleegd via https://www.uwv.nl/werkgevers/Images/handleiding-ontslagaanvraag-wegens-bedrijfseconomische-redenen.pdf

Wat is een Burgerservicenummer (BSN)?
Het Burgerservicenummer (BSN) is een uniek nummer en wordt beschouwd als een persoonsgegeven van gevoelige aard. Het is oorspronkelijk bedoeld voor de communicatie tussen burgers en de overheid. Andere organisaties mogen het BSN uitsluitend gebruiken als dat wettelijk is bepaald. Het gebruik van een BSN is aan strikte regels gebonden en de Autoriteit Persoonsgegevens treedt actief op tegen verkeerd gebruik.

Welke organisaties mogen mijn Burgerservicenummer (BSN) gebruiken?
Alle overheidsorganisaties mogen gebruik maken van uw burgerservicenummer (BSN). Andere organisaties mogen uw BSN gebruiken als dit in een wet staat.
https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/vraag-en-antwoord/welke-organisaties-mogen-mijn-burgerservicenummer-bsn-gebruiken

Waar kan ik een overheidsorganisatie opzoeken?
https://almanak.overheid.nl/

Mogen organisaties het BSN van klanten, relaties en werknemers overal voor gebruiken?
Nee, want het gebruik van iemands' BSN is aan strikte regels gebonden. Een werkgever mag het Burger Service Nummer (BSN) van werknemers niet gebruiken voor de toegangscontrole in het kantoorpand. Op een bedrijventerrein mogen leveranciers niet worden gevraagd om hun BSN. Bij de inschrijving van een kandidaat bij een uitzendbureau mag ook niet standaard gevraagd worden om het BSN. Een kopie van een paspoort maken bij autohuur of voor een abonnement op de sportschool zonder dat het BSN wordt weggestreept, is ook in strijd met de wet. Wanneer en hoe mag een BSN dan wel gebruikt worden?

Is TNO te beschouwen als ZBO c.q. overheidsorganisatie en mag deze dus het BSN nummer gebruiken c.q. kopie van belastingaangifte opvragen?
Ja, TNO is een Zelfstandig Bestuursorgaan (ZBO), voert overheidstaken uit en valt als overheidsorganisatie onder de Wet Openbaarheid van bestuur (WOB). Bijvoorbeeld opvragen kopie van de belastingaangifte. Op de belastingaangifte staat het BSN nummer.

Is TNO een ZBO?
Ja, TNO is per wet opgericht: https://wetten.overheid.nl/BWBR0003906/2019-01-01 . TNO is daarom een zogenaamd Zelfstandig Bestuursorgaan (ZBO).

Wat voor soort ZBO is TNO?
Of een orgaan een ZBO is wordt namelijk niet bepaald door de Kaderwet ZBO's, maar door de desbetreffende instellingswet, in casu de TNO-wet. Er bestaan twee soorten ZBO's, namelijk ZBO's zonder openbaar gezag en ZBO's met openbaar gezag. TNO is een ZBO zonder openbaar gezag die voor een substantieel deel wordt gefinancierd vanuit 's Rijks begroting.
https://zoek.officielebekendmakingen.nl/kst-25268-76.html

Is TNO als ZBO zonder openbaar gezag een overheidsorganisatie?
Een zelfstandig bestuursorgaan (zbo) voert een overheidstaak uit, zie: https://www.rijksoverheid.nl/onderwerpen/rijksoverheid/zelfstandige-bestuursorganen. Ook in jurisprudentie is TNO een bestuursorgaan in het kader van de WOB, zie: Raad van State, 2017-08-30, 201502714/1/A3, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RVS:2017:2334

Wat is AVG-compliant bij verstrekken BSN-nummer aan UWV voor ontslagaanvraag?
1. Verstrekken: Het verstrekken een lijst met BSN nummers van alle medewerkers ten behoeve van het UWV conform de wettelijke vereisten alleen kan plaatsvinden voor:
   - Aanvraagformulier deel A: een lijst met de namen, adressen en burger-servicenummers van de werknemers waarvoor een ontslagvergunning wordt gevraagd:
   - Aanvraagformulier deel B: NAW-gegevens werknemer, inclusief correspondentieadres en telefoonnummer; geboortedatum en Burgerservicenummer (BSN) werknemer. Alle privacygevoelige informatie over een werknemer dient u als een bijlage toe te voegen aan aanvraagformulier deel B van de betreffende werknemer, waarvoor een ontslagvergunning wordt gevraagd. Geef op die privacygevoelige informatie wel duidelijk aan bij welke vraag/antwoord deze informatie hoort.
   - Aanvraagformulier deel C: Alle privacygevoelige informatie over een werknemer dient u als een bijlage toe te voegen aan aanvraagformulier deel B van de betreffende werknemer, waarvoor een ontslagvergunning wordt gevraagd. Geef op die privacygevoelige informatie wel duidelijk aan bij welke vraag/antwoord deze informatie hoort.
   - In het geval van een datalek is het UWV zelfstandig verwerkingsverantwoordelijke en doet dus zelf melding van een datalek bij de Autoriteit Persoonsgegevens
2. Indienen:
   - De ontslagaanvraag moet via het account van de (formele) werkgever bij wie de werknemer in dienst is, worden ingediend.
   - De werkgever kan de ontslagaanvraag ook door een gemachtigde (bijvoorbeeld een advocaat) laten indienen. Daarvoor moet de gemachtigde via het werkgeversportaal bij de werkgever een machtiging aanvragen.

Wat is AVG non-compliant bij verstrekken BSN-nummer aan UWV voor ontslagaanvraag?:
Een lijst met de namen en burger-servicenummers van alle werknemers, dus inclusief de medewerkers waarvoor geen ontslagvergunning wordt aangevraagd, is dus niet wettelijk toegestaan. Het wel verstrekken betekent een non compliance in het kader van de Algemene Verordening Gegevensbescherming

Spelregels voor fiscale dienstverleners?
Fiscale dienstverleners hebben het BSN-nummer van hun cliënten vrijwel altijd nodig om een opdracht goed te kunnen uitvoeren. Verder heeft de wetgever de plicht om een cliënt te identificeren – zoals voorgeschreven in de Wwft – benoemd tot 'zwaarwegende reden'. Dit zet een aantal privacyregels 'op de tweede plaats'. Daarom is het voor accountants-, administratie- en belastingadvieskantoren geen probleem om een kopie van het ID-bewijs te maken en dit op te slaan in het cliëntdossier. Het afplakken van gegevens is daarbij niet nodig. Uiteraard moet er wel vertrouwelijk en zorgvuldig worden omgegaan met de vastgelegde persoonsgegevens!

Mag werkgever een BSN delen met een leidinggevende in een eigen formulier, bijvoorbeeld voor bijhouden uren werktijdverkorting?
Nee, gebruik een alternatief uniek nummer bijvoorbeeld MAAS Personeelsnummer

- Het wettelijk vereiste formulier is Aanvraag WW-uitkering bij werktijdverkorting
- MAAS kan, onder voorwaarden, met het formulier 'Aanvraag WW-uitkering bij werktijdverkorting' een WW-uitkering aanvragen voor uw werknemers, wanneer er door omstandigheden minder werk is. In het formulier dienen naast BSN andere persoonlijke gegevens ingevuld te worden door werkgever en individuele werknemer.
- Het gebruik van het Burgerservicenummer bij het bijhouden door de leidinggevende van de gewerkte uren tijdens Werktijdverkorting ten behoeve van deeltijd WW is niet wettelijk bepaald, dus niet toegestaan

Welke gegevens mag het UWV bij tijdelijke WW-uitkering wegens werktijdverkorting verzamelen en verwerken?

- identiteit, zoals naam, Burgerservicenummer en adres
- geslacht en leeftijd
- het loon
- de uitkering, de hoogte hiervan en de periode waarop betrekken hierop recht heeft

UWV mag deze persoonsgegevens delen met:

- ministerie van Sociale Zaken en Werkgelegenheid
- Inspectie SZW

Bronnen:

- Beleidsregels Ontheffing verbod van werktijdverkorting 2004
- https://www.uwv.nl/avg-privacystatement/overzicht-van-persoonsgegevens-die-uwv-verwerkt/detail/ww-uitkering-wegens-werktijdverkorting
- https://www.uwv.nl/werkgevers/formulieren/index.aspx

90. Identificatie. Foto en film (inclusief cameratoezicht)

Wat zegt de Autoriteit Persoonsgegevens over foto en film:

- https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/foto-en-film
- https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/cameratoezicht/cameratoezicht-op-de-werkplek
- https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-inzicht-gebruik-camera%E2%80%99s-voor-beveiligen-eigendom#subtopic-1866
- https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-informeert-branche-over-norm-camera%E2%80%99s-reclamezuilen#subtopic-1727

Jurisprudentie:

- Ontslag op basis van camerabeelden
  https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBLIM:2019:2130
- Niet werkende camera
  https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHDHA:2018:2883

Wanneer is heimelijke controle van werknemers mogelijk?

Heimelijke controle is een verstrekkend controlemiddel, omdat het een ernstige inbreuk op het privacybelang van de werknemer(s) is. Bij heimelijke controle (zoals verborgen cameratoezicht op de werkvloer bij serieus vermoeden van bedrijfsdiefstal) gelden naast de hierboven genoemde voorwaarden, aanvullende eisen.

- Als werkgever kan je niet lichtvaardig besluiten tot een inzet van heimelijke controle. Hiervoor zal je een redelijke verdenking van een strafbaar feit gepleegd door een of meerdere werknemers moeten hebben, zoals diefstal.
- De inzet van heimelijke controle moet zo kort en gericht mogelijk zijn en incidenteel.
- Ook moet je het personeel informeren dat heimelijke controle kan plaatsvinden, wanneer en op welke wijze.
- Voordat je overgaat tot de inzet van een verborgen controlemiddel, zoals een verborgen camera, moet je kunnen aantonen dat je ondanks allerlei inspanningen geen einde hebt kunnen maken aan de diefstal of fraude.
- Ook moet een DPIA zijn uitgevoerd: ook hier geldt dat als uit de DPIA komt dat sprake is van een verhoogd risico op de inbreuk van de privacy van de werknemers en je geen maatregelen vindt om dat risico te verminderen, dat je dan eerst de AP moet raadplegen voordat je tot de heimelijke controle overgaat.

Gebruik camerabeelden ondanks verzet werknemer mogelijk?

Het staat buiten kijf dat de werkgever zich dient te houden aan de voorwaarden die de AVG en de UAVG stellen voor het controleren van zijn personeel. De AP controleert hier ook op en is bevoegd om in geval van schending een sanctie op te leggen.
Kantonrechters daarentegen leggen het verzet van de werknemer op onrechtmatige inbreuk op zijn privacy in een ontslagzaak nog wel eens terzijde, omdat de waarheidsvinding in dat geval prevaleert. Dat informatie van ingezette controlemiddelen, zoals camerabeelden, succesvol door de werkgever kan worden gebruikt ter onderbouwing van bijvoorbeeld de dringende reden van een ontslag op staande voet, is aan de orde geweest in een uitspraak van de kantonrechter. In die zaak liet de kantonrechter de camerabeelden toe, ondanks verzet van werknemer daartegen.
Naar aanleiding van die beelden heeft werkgever werknemer ontslag op staande voet verleend. Werknemer verzet zich tegen dit ontslag. Hij stelt dat de camerabeelden uit de zaak moeten worden gehouden, omdat deze een onrechtmatige inbreuk op zijn privacy maken. De beelden zijn namelijk

zonder zijn toestemming gemaakt en over het plaatsen van de camera is geen instemming van de OR.
De kantonrechter gaat hieraan voorbij door te oordelen dat de waarheidsvinding in deze prevaleert boven het privacybelang van werknemer. De verdenking is ernstig en serieus (qua omvang), het bedrijfsbelang van werkgever (bescherming bedrijfseigendommen) is ontegenzeggelijk groot en met de camera is slechts op twee plekken gefilmd voor dat specifieke doel en dat is niet langer gedaan dan noodzakelijk. Daarbij heeft werkgever weken voorafgaand aan de inzet van de camera in een personeelsbijeenkomst melding gemaakt van de verdenking en het personeel gewaarschuwd.
Op basis van de camerabeelden en het feit dat werknemer onvoldoende de verdenking op de verduistering weerspreekt, blijft het gegeven ontslag op staande voet in stand.

Voorwaarden AVG voor camera
Als op de camerabeelden natuurlijke personen te zien zijn die geïdentificeerd zijn of kunnen worden, dan zijn de voorwaarden van de AVG in beginsel van toepassing. Dat is ook zo als de camera's draaien zonder de beelden op te slaan, maar niet als de camera's niet draaien.
Dat laatste komt voor. Denk aan de aanwezigheid van bewakingscamera's die niet werken. De AVG is dan niet van toepassing en van een inbreuk op de privacy is dan geen sprake.

Maakt iemand foto's en filmpjes voor zichzelf?
Dan geldt de privacywet niet. Er is namelijk een uitzondering voor persoonlijk of huishoudelijk gebruik (ook wel de 'huishoudelijke exceptie' genoemd). De voorwaarde hierbij is dat deze persoon de foto's en filmpjes privé houdt of hooguit in een zeer beperkte kring deelt. Bijvoorbeeld in een kleine appgroep. De gegevens mogen dus niet openbaar zijn voor iedereen (ook niet voor 'vrienden van vrienden' op Facebook). Via zoekmachines mogen de gegevens ook niet te vinden zijn. Op Facebook kun je instellen dat uw profiel alleen toegankelijk is voor uw vrienden. Dit doet u via de privacy instellingen. Bij een privé weblog of website kunt je bijvoorbeeld een verplicht wachtwoord instellen en de pagina's met persoonsgegevens afschermen voor zoekmachines.

Wat is de bewaartermijn voor camerabeelden?
Voor camerabeelden geldt een bewaartermijn van 4 weken. Maar als zich in die periode een incident voordoet (bijvoorbeeld winkeldiefstal) mag u de beelden bewaren totdat het incident volledig is afgewikkeld. U heeft daar dan een gerechtvaardigd belang bij.

Is het heimelijk opnemen van telefoongesprekken van medewerkers toegestaan?
In het geheim opnemen van een telefoongesprek is alleen toelaatbaar bij bedreigingen, bommeldingen en bij verdenking van strafbaar gedrag, zoals het naar buiten brengen van bedrijfsgeheimen. U mag dit alleen doen als een andere, minder ingrijpende wijze niet meer mogelijk is.
Bij geheime opnames moet u voldoende waarborgen treffen, zoals de verhindering van onrechtmatige toegang tot de opnames, en zo spoedig mogelijk vernietiging van de opnames bij afwezigheid van strafbaar gedrag.
Telefoongesprekken van medewerkers opnemen is slechts toegestaan als u daarbij een gerechtvaardigd belang heeft, bijvoorbeeld bij verdenking van fraude. U dient een privacytoets uit te voeren. Dit betekent dat u de belangen van de medewerker in kwestie moet afwegen tegen uw belang bij het opnemen van telefoongesprekken. U moet de betrokken medewerker(s) van tevoren informeren over het opnemen.

Hoe lang mag ik de opnames van telefoongesprekken bewaren?
In het algemeen geldt dat opnames van telefoongesprekken niet langer bewaard mogen worden dan noodzakelijk, bij voorkeur niet langer dan zes maanden.

Mag ik een verborgen camera op de werkplek installeren om bijvoorbeeld diefstal op te helderen?
In principe mag een werkgever geen gebruik maken van een verborgen camera, omdat dit een inbreuk vormt op de privacy van de medewerker. Maar als u een gerechtvaardigd belang heeft, mag het wel. Dit is het geval wanneer alle andere manieren om diefstal op te helderen zijn mislukt. Daarnaast moet het cameratoezicht noodzakelijk zijn. Als de werkgever het doel op een andere manier kan bereiken, dan gaat hier de voorkeur naar uit. Het cameratoezicht mag alleen voor korte periodes worden ingezet, moet gericht plaatsvinden en beperkt blijven tot incidentele gevallen.
Let op! Het is van belang om een regeling op te stellen over het gebruik van (verborgen) camera's. De ondernemingsraad heeft hierover instemmingsrecht. Daarnaast moeten het personeel en de ondernemingsraad hierover worden geïnformeerd.

Als ik de medewerkers vooraf informeer, dan zal het verborgen cameratoezicht weinig zin hebben. Hoe omzeil ik dat?
U kunt in de arbeidsovereenkomst daarover een clausule opnemen. Bijvoorbeeld dat er steekproefsgewijs controles plaatsvinden en dat u het recht voorbehoud om hierbij gebruik te maken van een verborgen camera.

Hoe lang mag ik de beelden bewaren?
De beelden mogen niet langer dan vier weken worden bewaard. Maar als zich in die periode een incident voordoet (bijvoorbeeld winkeldiefstal), mag u de beelden bewaren totdat het incident is afgewikkeld.

Wat kan er gebeuren als er niet aan alle wettelijke vereisten is voldaan?
U riskeert dat een rechter in een procedure de beelden kwalificeert als onrechtmatig verkregen bewijs en deze niet gebruikt mogen worden tegen de medewerker. Als de ondernemingsraad geen instemming heeft verleend, kan zij de nietigheid van het besluit inroepen binnen één maand nadat het besluit is genomen, of nadat de ondernemingsraad van het besluit wist of had kunnen weten. Nietigheid betekent in dit geval dat de camera's verwijderd moeten worden en de opgenomen beelden idem.

Wat zijn personeelsvolgsystemen?
Dit is het volgen van personeel via een geautomatiseerd systeem, zoals prikklok, pieper, controlecamera's, badges, e.d. Er zijn ook systemen die niet bedoeld zijn voor het volgen van personeel, maar wel als zodanig gebruikt kunnen worden. Denk aan beveiligingscamera's, GPS, chipkaarten en telefoonopnamen.

Waar moet ik rekening mee houden bij het invoeren van een personeelsvolgsysteem?
Als er een ondernemingsraad aanwezig is, heeft deze instemmingsrecht met betrekking tot de invoering, wijziging of intrekking van een regeling over een personeelsvolgsysteem. U moet altijd nagaan of deze verwerking van persoonsgegevens een legitiem doel heeft. U moet ook nagaan of er andere manieren zijn die minder verstrekkend zijn, gelet op de privacy van de werknemer. De gegevens mag u niet langer bewaren dan noodzakelijk is en u moet de gegevens zorgvuldig bewaren en zorgvuldig vernietigen als deze niet meer nodig zijn.

Hoe informeer ik mijn medewerkers over een regeling inzake een personeelsvolgsysteem?
Voor de gebondenheid door de medewerkers aan de regeling kunt u het beste bij indiensttreding de medewerker de regeling laten ondertekenen. Of u kunt in de arbeidsovereenkomst vermelden dat de regeling integraal onderdeel uitmaakt van de arbeidsverhouding. Voor de gebondenheid is niet voldoende dat de ondernemingsraad heeft ingestemd met de regeling.

De ondernemingsraad heeft ingestemd met het gebruik van GPS op de voertuigen. Mag ik de verkregen informatie ook gebruiken voor beoordeling van de medewerkers?
Nee, u mag deze persoonsgegevens nergens anders voor gebruiken dan waarvoor zij zijn bedoeld. En dus mogen de gegevens niet gebruikt worden als controlemiddel van het functioneren van de medewerker.

91. Identificatie. Identiteitsbewijs

Wat zegt de Autoriteit Persoonsgegevens over kopie identiteitsbewijs:
Zie: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/identificatie/identiteitsbewijs

Welke organisaties mogen een kopie van mijn identiteitsbewijs maken?
Slechts enkele organisaties mogen een kopie van een identiteitsbewijs maken. Eigen werkgever, overheidsinstanties, banken, notarissen, casino's en levensverzekeraars mogen dit bijvoorbeeld. Het bedrijf of de organisatie moet u informeren over de wettelijke verplichting In de praktijk vragen ook andere organisaties een kopie van uw legitimatiebewijs. Je bent niet verplicht om die aan hen te geven.

Valt het laten tonen of tijdelijk innemen van een identiteitsbewijs onder de AVG?
Nee, bij het laten tonen of tijdelijk innemen van een identiteitsbewijs verwerkt een organisatie geen persoonsgegevens. Daarom vallen deze situaties niet onder de AVG. Maar er kunnen wel andere (wettelijke) regels gelden. Zo moeten mensen op grond van de *Wet op de identificatieplicht* in bepaalde situaties hun identiteitsbewijs laten zien. Een identiteitsbewijs blijft altijd eigendom van de staat.

92. Identificatie. Overeenkomst met persoonsgegevens voor toegangspas

Mogen MAAS medewerkers de eigen persoonsgegevens ten behoeve van een toegangspas bij een klant wel doorgeven?
Ja, de klant gaat in dit geval geen persoonsgegevens voor MAAS International B.V. verwerken, maar wel persoonsgegevens van MAAS medewerker(s) voor eigen doeleinden verwerken. De klant is dus zelfstandig Verwerkingsverantwoordelijke in het kader van de AVG.

93. Identificatie. Receptie/ bezoekers

Vanaf 1 juni 2018 ontvangen MAAS bezoekers geen bezoekersbadge meer van de receptioniste. Alle bezoekers worden geregistreerd via het bezoekersregistratieformulier. Deze is te vinden op de balie **van** de receptie. Bezoekers worden vriendelijk verzocht om zich in- en uit te schrijven.

Wie is verantwoordelijk voor bezoek en uitschrijven.
MAAS medewerkers hebben de verantwoordelijkheid voor het eigen bezoek. Dit houdt in dat MAAS medewerkers alle bezoekers zelf ontvangen en ook bij het weggaan meelopen naar beneden.

Hoe lang is de bewaartermijn van de bezoekersgegevens?
In het verwerkingsregister is aangegeven om welke reden en hoe lang de bezoekersgegevens worden bewaard.

94. Identificatie. Uitzendkrachten

Wat zegt de Autoriteit Persoonsgegevens over kopie identiteitsbewijs:
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/identificatie/identiteitsbewijs#mag-ik-als-uitlener-of-onderaannemer-het-bsn-van-mijn-werknemer-aan-de-inlener-of-aannemer-verstrekken-6002

Wat zijn de regels voor kopie identiteitsbewijs voor uitzendkrachten
De Wet allocatie arbeidskrachten door intermediairs (Waadi) is per 1 januari 2018 gewijzigd ten aanzien van het maken en bewaren van een kopie van het identiteitsbewijs van nog niet werkzame uitzendkrachten (kandidaten). Tot 1 januari 2018 was het niet toegestaan om bij inschrijving van een kandidaat direct een kopie van het identiteitsbewijs te maken en te bewaren. Dit was alleen toegestaan op het moment dat vaststond dat de uitzendkracht daadwerkelijk werkzaamheden ging verrichten.
De wijziging met ingang van 1 januari 2018 betekent dat een uitzendbureau direct bij inschrijving een kopie van het id-bewijs mag maken en maximaal vier weken mag bewaren. Deze wijziging is opgenomen in de Verzamelwet SZW 2018. Het idee hierachter is dat de uitzendonderneming voldoende tijd heeft om de identiteit te checken en daarnaast te controleren of de kandidaat wel in Nederland mag werken. Ook wordt hiermee voorkomen dat er opnieuw een kopie van het id-bewijs gemaakt moet worden zodra een bemiddeling is geslaagd waardoor het risico op identiteitsfraude of onzorgvuldige verwerking van de kopie vermindert. Indien de intermediair bij inschrijving van kandidaten direct een kopie maakt en opslaat, dan mag deze kopie maar maximaal vier weken bewaard worden als een kandidaat uiteindelijk niet voor de intermediair gaat werken. Wanneer een kandidaat binnen deze vier weken aangeeft niet meer door intermediair bemiddeld te willen worden, moet intermediair de gegevens van deze kandidaat direct verwijderen uit de database.

Welke gegevens van de ingeleende werknemer moet Maas in de administratie opnemen om de identiteit van de werknemer te kunnen aantonen:

- naam-, adres- en woonplaatsgegevens;
- geboortedatum;
- burgerservicenummer (BSN);
- specificatie van de gewerkte uren;
- nationaliteit;
- soort identiteitsbewijs, nummer en geldigheidsduur;
- als dat van toepassing is, de aanwezigheid van een A1-verklaring, verblijfsvergunning, tewerkstellingsvergunning, notificatie of VAR-verklaring inclusief nummer en geldigheidsduur;
- naam-, adres- en woonplaats van de uitlener en het inschrijvingsnummer van de uitlener bij de Kamer van Koophandel.

U controleert het originele identiteitsbewijs van de ingeleende werknemer en neemt de gegevens over op het moment dat de ingeleende werknemer de (aanneem)overeenkomst gaat uitvoeren.

Hoe controleert Maas het originele identiteitsbewijs van de ingeleende werknemer om de gegevens over te nemen in de administratie?
Nu komen de uitzendkrachten lang niet allemaal fysiek bij Maas hoofdkantoor langs, dus ofwel de Maas leidinggevende controleert het originele identiteitsbewijs en neemt de gegevens over ofwel uitzendbureau verstrekt de gegevens op basis van onderstaande onderbouwing:

1. Maas doet géén beroep op de overeenkomst met de leasemaatschappij.
2. Maas heeft een Samenwerkingsovereenkomst met uitzendbureau. De gegevens zijn noodzakelijk voor de uitvoering van deze overeenkomst.

- Uitzendbureau conformeert in de Samenwerkingsovereenkomst aan het beleid en de besluiten van de ABU. Alleen aan het verstrekken van de BSN voorwaarde gesteld: Het BSN van de uitzendkracht mag alleen verstrekt worden aan de inlener mits dit noodzakelijk is voor vaststelling van de aansprakelijkheid (in het kader van de wet ketenaansprakelijkheid) van de inlener https://www.abu.nl/app/uploads/2019/02/Handreiking-privacy-Dos-en-Donts-versie-december-2017.pdf.pdf
- Uitzendbureau en inlener zijn ‘verwerkingsverantwoordelijke’. Inleners zijn géén verwerkers. Maas bepaalt zelf zijn doelen en middelen voor de gegevensverwerking. Maas beslist zelf met welke gegevensverwerkingssystemen wordt gewerkt, welke gegevens daarin worden opgenomen en op welke wijze dit wordt gedaan. Dit gebeurt niet in opdracht van Randstad en de inlener legt geen verantwoording aan Randstad af over zijn handelen ten aanzien van persoonsgegevens. Zowel de Randstad als Maas zijn daarom ‘verwerkingsverantwoordelijke’ en geen ‘verwerker’. Er hoeft dus géén verwerkingsovereenkomst te worden gesloten.

Je kunt Uitzendbureau dus op 2 manieren aanvliegen:

- Uitzendbureau verstrekt op basis van de Samenwerkingsovereenkomst alsnog de gevraagde gegevens aan zelfstandig verwerkingsverantwoordelijke Maas
  ofwel
- Uitzendbureau vertrekt een schriftelijk onderbouwd bezwaar van de Functionaris Gegevensbescherming van Randstad,

FG Maas zal een formeel bezwaar van FG Uitzendbureau vervolgens met de Autoriteit Persoonsgegevens zal bespreken. Indien AP:

- FG Maas gelijk geeft, dan dient Uitzendbureau de gegevens alsnog te verstrekken
- FG Uitzendbureau gelijk geeft, dan krijgen de directe leidinggevenden van Maas er een taak bij

95. Identificatie. Wet Arbeid Vreemdelingen

Wat is de WAV?
Artikel 2 van de Wet arbeid vreemdelingen verbiedt werkgevers een vreemdeling in Nederland arbeid te laten verrichten zonder tewerkstellingsvergunning.
Artikel 15 van de Wet arbeid vreemdelingen stelt een zorgplicht voor werkgevers vast om, in het geval dat een vreemdeling arbeid feitelijk gaat verrichten bij een andere werkgever, die andere werkgever een afschrift van een document ter identificatie van die vreemdeling te overleggen.

Vreemdeling in de zin van de WAV zijn onderdanen van buiten de Europese Economische Ruimte (EER) en Zwitserland. Het gaat dus om mensen die van buiten de EER komen. De EER bestaat uit: België, Bulgarije, Cyprus, Denemarken, Duitsland, Estland, Finland, Frankrijk, Griekenland, Hongarije, Ierland, IJsland, Italië, Kroatië, Letland, Liechtenstein, Litouwen, Luxemburg, Malta, Nederland, Noorwegen, Oostenrijk, Polen, Portugal, Roemenië, Slovenië, Slowakije, Spanje, Tsjechië, Verenigd Koninkrijk en Zweden.

Mag een klant bij Maas een steekproef doen op de WAV (wet arbeid vreemdelingen)?
Ja, dat is toegestaan, waarbij je een zogenaamd afschrift stuurt dus kopie uit de loonadministratie. Hierop mag geschreven zijn of een markering zijn aangebracht, zolang de gegevens duidelijk leesbaar zijn. Grondslag van de verwerking is het voldoen aan een wettelijke verplichting.
Indien van klant geen getekende Maas Verwerkingsovereenkomst is (Maas verwerkingsverantwoordelijke en klant verwerker), dan is de klant zelfstandig Verwerkingsverantwoordelijke bij een (ernstige) datalek bij hun van deze persoonsgegevens.
ere toelichting:

Hoe verstrek je de documenten van een zogenaamde vreemdeling (WAV)?

- *Geldig legitimatiebewijs, te interpreteren als "afschrift geldig paspoort met een officiële sticker van de IND, met daarop de aantekening 'Arbeid is vrij toegestaan. Tewerkstellingsvergunning (TWV) niet vereist'*
    - Duur van document
    - Leesbaarheid document
    - Einddatum document juist verwerkt in administratief systeem
- *Verblijfsvergunning, te interpreteren als "afschrift" van geldig verblijfsdocument met daarop de aantekening 'Arbeid is vrij toegestaan. Tewerkstellingsvergunning (TWV) niet vereist.'*
    - Duur van document
    - Leesbaarheid document
    - Einddatum document juist verwerkt in administratief systeem
- *Tewerkstellingsvergunning TWV, te interpreteren als "afschrift" geldige tewerkstellingsvergunning (TWV) voor deze persoon*
    - Duur van document
    - Leesbaarheid document
    - Einddatum document juist verwerkt in administratief systeem

Wanneer verstrek je een Tewerkstellingsvergunning (TWV) voor een EU langdurig ingezetene?
Voor vreemdelingen die in een andere (EU) lidstaat de status langdurig ingezetene hebben verkregen en vervolgens in Nederland een verblijfsvergunning voor (EU) langdurig ingezetenen krijgen, is in het eerste jaar van dit verblijf een tewerkstellingsvergunning nodig die moet worden aangevraagd door hun werkgever. Zij vragen geen gecombineerde vergunning voor verblijf en arbeid aan.

Na ten minste één jaar legaal in Nederland verblijf als langdurig ingezeten onderdanen van derde landen mag dus geen tewerkstellingsvergunning of gecombineerde vergunning worden verlangd.

- https://wetten.overheid.nl/BWBR0034945/2018-09-04 (Regeling uitvoering Wet arbeid vreemdelingen 2014), specifiek:
    - Bijlage I. Uitvoeringsregels, behorende bij de artikelen van de Regeling uitvoering wet arbeid vreemdelingen 2014. Inleiding Regeling uitvoering Wet arbeid vreemdelingen 2014 en bijbehorende Uitvoeringsregels
    - Bijlage II Mededeling als bedoeld in artikel 3, tweede lid, van de Wet arbeid vreemdelingen
- https://ind.nl/onbepaalde-tijd/Paginas/Aanvragen-status-EU-langdurig-inzetene.aspx v

Hoe verstrek je de documenten van een zogenaamde langdurig ingezetene?

- Verblijfsvergunning, te interpreteren als “afschrift” van geldig verblijfsdocument langdurig ingezetene

Alleen in eerste jaar is aanvullend nodig:

- Tewerkstellingsvergunning TWV, te interpreteren als “afschrift” geldige tewerkstellingsvergunning (TWV) voor deze persoon

Is MAAS verplicht een geldig document in de administratie op te slaan, of is het voldoende als het document geldig was op het moment van indiensttreding?

Antwoord is nergens eenduidig aangegeven, dus gebruiken we de FAQ info van de IND.
Vraag om een nieuwe kopie bij de langdurig ingezetene. Nieuwe vergunning is namelijk binnen 2 jaar na verlopen van de oude “bepaalde tijd” verplicht.
Mijn verblijfsvergunning is verlopen. Wat kan ik doen?
Als uw verblijfsvergunning is verlopen, moet u zo snel mogelijk een verlengingsaanvraag indienen. Omdat u de aanvraag indient na het verlopen van uw verblijfsvergunning, krijgt u een mogelijk een verblijfsgat.
U kunt dit doen tot een redelijke termijn van 2 jaar na het verlopen van uw vergunning. Is uw verblijfsvergunning langer dan 2 jaar verlopen? De IND wijst uw verlengingsaanvraag dan af.
Hebt u een verlengingsaanvraag ingediend? Dan kunt u een verblijfsaantekening aanvragen bij het IND-loket. De verblijfsaantekening is een sticker in uw paspoort. Met deze sticker kunt u laten zien dat u in Nederland mag wonen.
Hebt u geen paspoort? En kunt u deze ook niet krijgen? U kunt een Vreemdelingen Identiteitsbewijs aanvragen.
Bron: https://ind.nl/Paginas/Verlengen-verblijfsvergunning.aspx

Wat moet ik (werknemer) doen als ik bij een andere werkgever ga werken?

Als u van werkgever verandert, dan moet u of uw werkgever dit melden aan de IND. Of u een nieuwe verblijfsvergunning moet aanvragen, hangt af van de verblijfsvergunning die u hebt. En of u bij uw nieuwe werkgever nog steeds aan de voorwaarden voor uw verblijfsvergunning voldoet.
Hebt u een verblijfsvergunning kennismigrant, Europese blauwe kaart, overplaatsing binnen een onderneming (ICT-richtlijn), wetenschappelijk onderzoeker (richtlijn 2005/71/EG) of onderzoeker (richtlijn (EU) 2016/801) dan hoeft de wijziging van werkgever alleen gemeld te worden. U moet wel aan de voorwaarden van uw verblijfsvergunning blijven voldoen.
Hebt u een verblijfsvergunning voor verblijf en arbeid (GVVA)? U of uw werkgever moet een nieuwe aanvraag indienen. Alle bewijsmiddelen moeten opnieuw worden bijgevoegd. De IND vraagt tijdens de aanvraag opnieuw aan UWV of u aan de kenmerken van de Wet arbeid vreemdelingen voldoet. Is het advies van UWV positief en uw verblijfsvergunning is nog langer dan 3 maanden geldig? U krijgt alleen een nieuw aanvullend document. Is uw verblijfsvergunning nog minder dan 3 maanden geldig? u krijgt een nieuwe verblijfsvergunning en een nieuw aanvullend document.

Hebt u een verblijfsvergunning arbeid in loondienst (niet GVVA)? Uw nieuwe werkgever moet een nieuwe tewerkstellingsvergunning (TWV) aanvragen bij UWV. Hebt u 5 jaar onafgebroken gewerkt? Dan bent u vrij om te werken in Nederland. U hebt geen TWV meer nodig. Laat uw werkgever altijd informeren bij UWV of een TWV nog nodig is.
Bron: https://ind.nl/contact/Paginas/Veelgestelde-vragen.aspx

96. Klantcontact. Cold calling/ Koude acquisitie

Wat zijn openbare gegevens?
Er zijn gegevens die je gemakkelijk op internet kunt vinden. Bijvoorbeeld op de contactpagina van een bedrijf, in een bedrijvengids, bij interviews, in een online folder of op LinkedIn. Deze gegevens zijn met een bepaald doel openbaar gemaakt. Deze gegevens mogen alleen gebruikt worden voor het doel waarvoor ze openbaar zijn gemaakt.

Is handel in gegevens toegestaan?
Adressenbestanden kun je ook gewoon kopen of huren. Handig, want zo hoef je zelf niet op zoek. Let wel op! De gegevens in deze bestanden, moeten net zo goed met een gerechtvaardigd doel zijn verzameld en deze gegevens mogen alleen gebruikt worden voor het doel waarvoor ze zijn verzameld. Heel vaak zijn deze gegevens wel verleend aan een bedrijf, maar niet met de bedoeling dat ook andere bedrijven dit mochten gebruiken. Controleer dit dus altijd wanneer je gebruik wil maken van zo'n bestand.

Kan ik de verkoper van adressenbestanden vragen hoe hij aan zijn gegevens komt?
Dit is inderdaad aan te bevelen. Vraag in ieder geval tenminste om een juridische borging dat de gegevens rechtmatig aan je mochten worden verstrekt voor de gevraagde doeleinden

Mag je zomaar iedereen opbellen?
Nee. Waar je op moet letten is met welk doel gegevens zijn gepubliceerd of ten behoeve van welk doel ze zijn verstrekt. Alleen als dat doel overeenkomt met het doel waar jij de gegevens voor wil gebruiken, is de koude telefonische acquisitie toegestaan.

Mag je alle openbare gegevens gebruiken?
Dat gegevens te vinden zijn op LinkedIn of op een website, wil nog niet zeggen dat je ze ook mag gebruiken. Gegevens op een website, zijn meestal bedoeld zodat klanten deze kunnen gebruiken om contact op te nemen, maar niet om gebeld te mogen worden zodat ze zelf ergens klant kunnen worden. Let daarom eventueel op de tekst bij de gegevens. Daaruit kun je vaak opmaken waarom de gegevens gepubliceerd zijn en waar ze voor gebruikt mogen worden. Dat er niet zoiets bij staat als 'acquisitie wordt niet op prijs gesteld', wil dus nog niet zeggen dat je wel zou mogen bellen. Je zou om de persoonsgegevens heen kunnen werken. Algemene bedrijfsgegevens zijn natuurlijk geen persoonsgegevens. Als je wel de naam hebt van de persoon die je wil bereiken, mag je dus wel het algemene nummer bellen van het bedrijf of van de betreffende afdeling. De persoon die opneemt kan je dan wel doorverbinden. Als het telefoontje wordt aangenomen, mag je vervolgens gewoon je verhaal houden.

Cold calling, mag dat nog wel?
Voor B2B-marketeers, die telefonische acquisitie (laten) doen, veranderen er twee belangrijke zaken. Zowel het directe telefoonnummer als het persoonlijke e-mailadres vallen per 25 mei 2018 onder persoonsgegevens. De naam van een persoon valt onder de wet, waardoor je in de praktijk niet meer mag vragen naar "Jan Jansen", maar alleen naar "de Facilitair Manager". Volgens de strikte letter van de wet mag je dus niet meer werken met vooraf verzamelde bestanden met namen en e-mailadressen van specifieke personen binnen bedrijven. Echter, als je toestemming hebt gekregen om iemand te mailen of te bellen op een specifiek nummer, dan is dat uiteraard gewoon toegestaan. In de praktijk geldt zoals altijd dat de toon de muziek maakt. Dus als je op een correcte wijze en open en eerlijk een relevante boodschap aan een persoon overbrengt en je respecteert zijn of haar (of een collega's) wens voor geen verdere contact, dit in de praktijk geen problemen zal

opleveren. Net zoals het nu bij de huidige regels voor het toesturen van e-mail geldt. Zorg dus voor een relevante boodschap en zorg voor een goede, snelle opt-out

Waar valt koude acquisitie onder in de nieuwe wet?
Binnen de AVG valt koude acquisitie of cold calling onder de term 'direct marketing'

Mag je direct marketing bedrijven bij bestaande klanten?
U mag uw eigen, bestaande klanten digitale direct marketing sturen met aanbiedingen voor andere, vergelijkbare producten of diensten. Bijvoorbeeld per e-mail, sms of app. Uw klanten hoeven daarvoor niet eerst toestemming te geven, maar u moet ze wel bij het bestelproces hebben gemeld dat u dit gaat doen en ze een afmeldmogelijkheid (opt-out) hebben gegeven.
Iemand is een bestaande klant als deze persoon een product of dienst van u heeft gekocht. Er moet sprake zijn van een koopovereenkomst, waarin u verplicht bent of was om iets te leveren en de klant om daarvoor te betalen. U mag iemand niet tot uw bestaande klanten rekenen als diegene (nog) niets heeft gekocht, maar zich alleen maar heeft aangemeld voor uw nieuwsbrief, een enquête heeft ingevuld, meegedaan heeft aan een prijsvraag of spel of een gebruikersaccount heeft aangemaakt.

Mag je direct marketing bedrijven bij niet-bestaande klanten?
Is iemand nog geen bestaande klant van u? En wilt u deze persoon mailen, sms-en of appen met aanbiedingen? Dan moet u diegene hiervoor eerst toestemming vragen.

Is er nog andere wetgeving van belang bij koude acquisitie?
Ja, ook de Telecommunicatiewet is van belang, omdat koude acquisitie het ongevraagd versturen van commerciële berichten betreft. De Telecommunicatiewet stelt ook regels ten aanzien van het ongevraagd telefonisch en per e-mail benaderen van potentiële klanten, met als doel goederen of diensten aan te bieden of te verkopen of denkbeelden te promoten. Telemarketing ten aanzien van consumenten en eenmanszaken is toegestaan, tenzij de ontvanger hier bezwaar tegen heeft gemaakt ('Bel-mij-niet'-register). Dit geldt niet ten aanzien van de BV, NV of stichting. Deze rechtspersonen mag je gewoon telefonisch benaderen, zolang je maar niet vraagt naar een specifieke persoon. Wat wel kan: een bedrijf bellen en vragen naar iemand die over marketing gaat.

Koude acquisitie gericht op bedrijven is dus niet verboden?
Nee, maar het hiervoor gebruiken van openbare bedrijfsgegevens is vaak wel verboden. Let er dus op dat:
•Bij het telefonisch benaderen van een bedrijf, je het algemene telefoonnummer gebruikt en niet vraagt naar een specifieke persoon, als je geen toestemming hebt gekregen van die persoon om hem of haar te benaderen;
•Bij het elektronisch (bijv. per e-mail) benaderen van een bedrijf je enkel gebruik maakt van een e-mailadres dat beschikbaar gesteld is voor acquisitie;
•Bij het verkrijgen van persoonlijke contactgegevens je expliciet toestemming verkrijgt om deze (op een later tijdstip) te gebruiken voor acquisitie. Let op dat je achteraf moet kunnen bewijzen dat je die toestemming hebt gekregen.
Cold callers zijn gewend om vanuit openbare bronnen gegevens te verzamelen van hun potentiële klanten, voordat ze contact opnemen. Ze gaan bijvoorbeeld op zoek op de website van de klant of kijken op Linkedin. Ze proberen zo de naam, functie of telefoonnummer van een contactpersoon te achterhalen. Mag je zondermeer dit soort gegevens opzoeken en opslaan in je eigen CRM-pakket, met als doel om deze later te gebruiken voor koude acquisitie?
Nee, het is niet toegestaan om zomaar gegevens uit externe bronnen in je CRM pakket te stoppen om daarmee acquisitie te plegen. Dat de bron openbaar was, is niet relevant. Waar het om gaat, is of

je een grondslag hebt om de acquisitie te doen. Dat kan zijn toestemming of een bestaande relatie. Maar “het staat al op internet” is geen grond.

Cold callers hebben vaak een zorgvuldig opgebouwde database, waarin door de jaren heen persoonsgegevens uit allerlei bronnen zijn verzameld. Denk aan gegevens van bedrijven waar in de afgelopen jaren acquisitie-acties zijn geprobeerd, die niet succesvol waren, (delen van) gekochte adressenbestanden en deskresearch uit openbare bronnen. Meestal is niet meer duidelijk waar gegevens überhaupt vandaan kwamen. Mogen dit soort gegevens gewoon gebruikt blijven worden, of moeten deze onder de AVG gegevens worden ‘opgeschoond’ of verwijderd?
Ook gegevens die je al had voordat de AVG van kracht werd, moeten vanaf 25 mei voldoen aan de eisen uit de AVG. Persoonsgegevens waarvan je niet kunt aantonen dat je ze met een AVG-proof grondslag hebt verkregen, moeten dus vernietigd worden.

In Overweging 47 van de AVG staat: “De verwerking van persoonsgegevens ten behoeve van direct marketing kan worden beschouwd als uitgevoerd met het oog op een gerechtvaardigd belang”. Het lijkt alsof je hiermee als verwerker van persoonsgegevens de afweging moet maken tussen de belangen van de verwerkende organisatie (jij als cold caller dus) en de privacy-belangen van je potentiële klant. Betekent dit dat je als cold caller bij iedere potentiële klant kunt zeggen: “Ik heb een afweging gemaakt en ik vind mijn belang groter dan het privacy-belang van mijn potentiele klant?” Simpel gesteld: mag ik als cold caller gewoon al mijn potentiële klanten bellen, omdat ik altijd mijn belang boven die van de klant laat gaan?
Naast toestemming en de contractuele relatie kent de AVG ook als grondslag het eigen gerechtvaardigd belang. Je zegt dan, mijn belang weegt zwaarder dan uw privacy dus ik mag dit gewoon doen. Inderdaad wordt direct marketing gezien als zo’n belang, maar je moet nog steeds laten zien waarom jouw behoefte aan direct marketing zwaarder weegt dan de privacy van de persoon die je benadert. Hieraan kun je voldoen door waarborgen in te bouwen, zoals een afmeldmogelijkheid. Maar je zult ook moeten aangeven waarom het legitiem is om die op internet gevonden gegevens te gebruiken voor direct marketing. Deze belangenafweging moet je op papier zetten zodat je achteraf bewijs hebt dat je er goed over nagedacht hebt vanuit jouw bedrijfssituatie.

Hoe zit het nu precies met het wel of niet direct vragen naar een bepaalde contactpersoon als je het algemene nummer belt van een bedrijf. Ga er hierbij vanuit dat je nog geen toestemming hebt gehad en de naam (dhr Jansen, hoofd afdeling marketing) in een openbare bron hebt gevonden. Kun je wel gewoon direct naar dhr Jansen vragen of mag je dan alleen vragen naar iemand die gaat over marketing?
De AVG gaat verder. Het feit dat Jansen in jouw CRM systeem zit, maakt dat je op dat moment al moet kunnen rechtvaardigen dat je dit doet. Heb je toestemming van Jansen, is er een contractuele relatie of heb je zo’n gerechtvaardigd belang? Als je Jansen op internet hebt gevonden, krijg je die rechtvaardiging niet snel rond.

Als je voor het eerst je potentiële klant aan de lijn krijgt, zijn er dan verplichtingen direct aan het begin van het gesprek? Bijvoorbeeld dat je meteen moet vertellen dat je zijn naam uit openbare bron hebt gevonden? Of zijn er andere zaken die je direct openbaar moet maken, ten aanzien van de AVG?
De AVG eist inderdaad dat je mensen actief informeert over hoe je aan hun gegevens komt en wat je daarmee doet. Dat hoef je niet als een robot direct aan het begin te doen, maar je moet het wel in het gesprek melden. Ook moet je mensen melden dat ze recht van bezwaar hebben, oftewel dat ze op verzoek uit jouw bestand verwijderd gaan worden.

In overweging 70 van de AVG staat: "Wanneer persoonsgegevens worden verwerkt ten behoeve van direct marketing dient de betrokkene, ongeacht of het een aanvankelijke dan wel een verdere verwerking betreft, het recht te hebben te allen tijde en kosteloos bezwaar te maken tegen deze verwerking, ook in het geval van profilering voor zover deze betrekking heeft op de direct marketing. Dat recht moet uitdrukkelijk, op duidelijke wijze en gescheiden van overige informatie, onder de aandacht van de betrokkene worden gebracht." Dit lijkt alsof je de potentiele klant erop moet wijzen dat je data opslaat in je CRM-systeem, als je hem of haar hebt benaderd via koude acquisitie. En dat de ander het recht heeft om toestemming te weigeren, zodat je verplicht bent deze data uit je CRM systeem te verwijderen. Hoe formeel moet je dit aanpakken? Is dit vergelijkbaar met het bekende bandje van de business to consumer callcenters, of kun je dit ook informeel in het gesprek verwerken?
Je bent verplicht inderdaad om ze te melden dat ze bezwaar kunnen maken, en je mag dat niet verstoppen in je algemene voorwaarden of website. Maar je mag het informeel in het gesprek melden, bijvoorbeeld zodra je merkt dat de gebelde persoon geen interesse heeft "Ach wat vervelend. Zal ik u dan meteen uit ons bestand halen ook, dat is namelijk uw wettelijk recht."

Hoe zit het met het direct benaderen van potentiële klanten op een platform als Linkedin. Je hebt hierbij de mogelijkheid om ongevraagd een zogenaamde 'inmail' te sturen. Valt deze manier van communicatie ook onder de AVG, is dit geregeld binnen de gebruiksovereenkomst van Linkedin of geldt hier iets anders?
Specifiek bij platforms als LinkedIn geldt dat je meer mag doen, wanneer het platform daar zelf expliciet functionaliteit voor heeft gebouwd. Zo kun je op LinkedIn instellen of je open staat voor bijvoorbeeld recruiters. Als je dat aangeeft, dan mag een recruiter je mailen, daar is die functionaliteit voor. Maar let op: je mag dan niet die persoon in je eigen database stoppen om hem later te blijven bestoken met nieuwe banen. Dat gaat buiten de functionaliteit van LinkedIn zelf om. LinkedIn heeft natuurlijk ook weer het recht om mensen te weren als die hun eigen huisregels overtreden. Het sociale netwerk verbiedt het versturen van "any unsolicited or unauthorized advertising, "junk mail," "spam," "chain letters," "pyramid schemes," or any form of solicitation unauthorized by LinkedIn;". Een koud acquisitiebericht kan daar eenvoudig onder vallen, en als LinkedIn genoeg klachten krijgt dan mogen ze je account afsluiten.

Als je toestemming hebt gekregen van een potentiële klant om hem of haar te benaderen, je deze toestemming (opt-in) moet vaststellen. Hoe zit dit als je mondeling toestemming hebt gekregen, hoe leg je dan deze opt-in vast? Neem bijvoorbeeld de situatie dat je iemand hebt gesproken op een netwerkbijeenkomst en je vraagt de ander of je hem kunt bellen om verder te praten over jouw product of dienst. Als de ander zegt dat dit oké is, dan heb je, neem ik aan, toestemming gekregen. Moet je deze toestemming dan vastleggen op een of andere manier?
Je moet onder de AVG inderdaad kunnen bewijzen dat je toestemming hebt. Beter gezegd: als je het niet kunt bewijzen dan wordt aangenomen dat je geen toestemming hebt. Je mag het aantonen zoals je wilt. Een gespreksopname is bijvoorbeeld prima bewijs, een notitie van een netwerkbijeenkomst zou ook aardig bewijs zijn.

Hoe zit het als een collega of bevriende relatie je aanraadt om eens contact op te nemen met een potentiële klant? Een praktijksituatie is bijvoorbeeld dat een bestaande klant je vertelt dat een relatie van hem ook gebruik zou kunnen maken van je producten of diensten. Hij geeft je hierbij meteen een naam en telefoonnummer. Heb je hiermee toestemming (opt-in) gekregen om te kunnen bellen?
In principe niet. Ik zou dus doorvragen, denk je dat hij het goed vindt dat ik hem direct bel? Als hij dan ja zegt, dan is dat in ieder geval een steviger argument naar die relatie toe waarom je hem belt.

Als een potentiële klant het zeer ongepast vond dat hij werd benaderd via koude acquisitie en het gevoel heeft dat zijn privacy hiermee is geschaad. Welke stappen kan hij nemen in de praktijk om bezwaar te maken?

De eerste optie is dus dat hij bij jou bezwaar kan maken, jij moet hem dan op de zwarte lijst zetten en je mag hem niet meer benaderen. Ook kan hij vragen hoe je aan zijn gegevens komt, en dan bij de bron gaan klagen of zorgen dat die zijn gegevens niet meer beschikbaar stelt.Als hij erg boos is, kan hij een klacht bij de toezichthouder (de Autoriteit Persoonsgegevens) indienen. Krijgen die genoeg klachten, dan starten ze een onderzoek tegen je en daar kan een boete uit volgen. Had je via e-mail, sms of telefoon hem benaderd, dan kan hij ook klagen bij de Autoriteit Consument en Markt wegens overtreding van de spamwetgeving. Ook daar kunnen boetes voor volgen als er genoeg klachten waren.

In theorie kan hij ook naar de rechtbank om een contactverbod te eisen op straffe van een dwangsom. Bel of mail je hem daarna toch, dan moet je bijvoorbeeld 500 of 1000 euro per bericht betalen. Dit is een paar keer gebeurd bij hardnekkige organisaties zoals de Postcode Loterij maar het is natuurlijk wel een dure stap om te nemen.

Als laatste blijft natuurlijk het aloude middel over van negatieve publiciteit: hij kan op Twitter of LinkedIn klagen dat hij steeds gebeld of gemaild wordt door een spammer.

97. Klantcontact. Cookie

Wat zegt de Autoriteit Persoonsgegevens over cookies?

- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies#mogen-organisaties-tracking-cookies-plaatsen-op-mijn-computer-2125
- https://autoriteitpersoonsgegevens.nl/nl/nieuws/websites-moeten-toegankelijk-blijven-bij-weigeren-tracking-cookies#subtopic-2077

Wat zegt de Autoriteit Co9nsument & Markt (ACM) over cookies?
https://www.acm.nl/nl/onderwerpen/telecommunicatie/internet/cookies

Hoe legt de AP de juridische normen rond cookiewalls uit?
https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_ap_cookiewalls.pdf

Welke wettelijke regels voor cookies
Voor het gebruik van cookies gelden wettelijke regels. Dat zijn in de eerste plaats regels uit de Telecommunicatiewet (Tw).
Maar op tracking cookies (in combinatie met overige gegevens die over het websitebezoek worden verzameld) is ook de Algemene verordening gegevensbescherming (AVG) van toepassing.
Uitleg over de wettelijke eisen aan andere soorten cookies is te vinden op de website van de Autoriteit Consument en Markt (ACM).

Mag een cookiewall (nog)?
De Autoriteit Persoonsgegevens (AP) gaf 7 maart 2019 een duidelijk statement: de cookiewall is onrechtmatig, bedrijven moeten bedrijfsproces aanpassen. Trackingcookies mogen pas geplaatst worden nadat daarvoor toestemming is gegeven door de websitebezoeker. Dat staat in de Telecommunicatiewet. De definitie van toestemming wordt geleend uit de Algemene Verordening Gegevensbescherming (AVG). Toestemming is dus pas geldig wanneer het aan de voorwaarden uit de AVG voldoet. Eén van die voorwaarden is dat de websitebezoeker ‘vrij’ moet zijn om toestemming te geven.

98. Klantcontact. Customer Care

Wat zegt de Autoriteit Persoonsgegevens over Customer Care?
Geen specifieke informatie

Moeten de rechten van klanten altijd gehonoreerd worden?
Klantenservicemedewerkers moeten wel echt precies weten welke rechten klanten en consumenten hebben en hoe zij die kunnen inwilligen. Een organisatie is namelijk beboetbaar als, al dan niet onbewust, de rechten van consumenten niet gehonoreerd worden.

Is het toegestaan om aankoop- en contacthistorie bij te houden?
Ja, waarbij klantcontactmedewerkers zich moeten afvragen of een bepaald gegeven bijdraagt aan het verbeteren van de dienstverlening. Dit geldt voor elk type persoonsgegevens, niet alleen voor bijzondere persoonsgegevens. Customer Care moeten gaan denken in ‘dataminimalisatie’.

Hebben klanten het recht om hun persoonsgegevens op te vragen?
Ja, dat hebben ze. Met de invoering van de AVG wordt het begrip dataportabiliteit ingevoerd. Een begrip dat wil zeggen dat degene van wie MAAS gegevens opslaat en verwerkt het recht heeft om eigen gegevens mee te nemen naar een andere partij. Klanten hebben het recht een kopie te ontvangen van de persoonsgegevens die MAAS heeft verzameld.
Het gaat om alle gegevens die klanten actief en bewust aan MAAS hebben verstrekt, zoals accountgegevens (e-mailadres, gebruikersnaam, etc.) die op een online formulier zijn ingevuld. En het gaat ook om gegevens die klanten aan MAAS hebben ‘verstrekt’ door MAAS diensten of apparaten te gebruiken. MAAS hoeft bij een verzoek om dataportabiliteit géén afgeleide gegevens te verstrekken, dat wil zeggen gegevens die MAAS zelf heeft gegenereerd door bijvoorbeeld data-analyse. Zoals een kredietscore of een profiel dat MAAS van een klant heeft opgesteld. Deze gegevens moet MAAS bij een inzageverzoek overigens wél verstrekken.

Hoe moet MAAS de persoonsgegevens aanleveren?
De gegevens moet u, op verzoek, aanleveren in een gestructureerd, veelgebruikt en machine leesbaar formaat. In andere woorden: de kopie moet in een algemeen gebruikt digitaal formaat worden aangeleverd zodat de bestanden verder gebruikt kunnen worden.

Mag ik kosten in rekening brengen voor dataportabiliteit?
Nee, in principe niet. Bij het recht op dataportabiliteit volgens de AVG mag MAAS geen geld vragen voor het verstrekken van kopieën. De kosten zijn voor rekening MAAS en mag MAAS niet verhalen op uw klanten of gebruiken als argument om een verzoek af te wijzen. Alleen als u kunt aantonen dat een verzoek duidelijk ongegrond is of excessief (bijvoorbeeld als u heel veel verzoeken van één persoon krijgt), kunt u geld vragen of het verzoek weigeren.

99. Klantcontact. Direct Marketing Prospects

Wat zegt de Autoriteit Persoonsgegevens over direct Marketing?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/direct-marketing

Hoe lang mag je gegevens van een prospect bewaren?
Dit is niet door de wet geregeld. Een onderneming moet zelf een bewaartermijn bedenken en onderbouwen waarom de gegevens voor die bewuste termijn worden bewaard.

Prospects benaderen MAAS proactief, wat moet bewaard worden?
De wettelijke bewaartermijn geldt. Als de prospect geen klant wordt, dan bepaalt de MAAS hoe lang er een noodzaak tot bewaren is.

Heb je toestemming nodig van de prospect om gegevens te bewaren?
Nee, dat is niet per se vereist. Wel dien je een prospect altijd te informeren over de vastlegging van diens gegevens in je systeem. Op dat moment moet de prospect ook geïnformeerd worden over het recht van bezwaar tegen die vastlegging.

Kan ik brieven versturen naar prospects?
Hier is geen toestemming voor nodig. Een prospect heeft altijd een recht van bezwaar achteraf mocht de direct marketing niet gewenst zijn.

Moet ik toestemming vragen voor een nieuwsbrief naar klanten en prospects?
Nee, dit is in beginsel niet nodig mits er sprake is geweest van adequate informatievoorziening. De Telecommunicatiewet regelt in artikel 11.7 het versturen van e-mailberichten. Voor meer uitleg wordt verwezen naar de website van de ACM.

Hoe moet een klant zich uitschrijven?
In elke nieuwsbrief of direct marketing uiting die op geautomatiseerde wijze wordt verzonden, dient een kenbare afmeldmogelijkheid te zijn opgenomen. Zie hiervoor hoofdstuk 11 van de Telecommunicatiewet.

Moeten oude klant/prospect bestanden opnieuw om toestemming gevraagd worden of de mogelijkheid van een opt out worden gegeven?
Nee, dit is in beginsel niet nodig. Als een klant of prospect geen berichten meer wilt ontvangen, dan kan deze altijd gebruik maken van de afmeldmogelijkheid.

Mogen prospects die bijvoorbeeld op een event ontmoet zijn, daarna zonder toestemming telefonisch benaderd worden?
Dit valt buiten het bestek van de AVG tenzij de belgegevens digitaal zijn vastgelegd.
Telefoongesprekken die handmatig worden gevoerd (dus niet met een belcomputer) mogen altijd zonder voorafgaande toestemming (‘cold calling’).

100. Klantcontact. Evenementen

Wat zegt de AP over Evenementen?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/foto-en-film/beeldmateriaal?qa=evenementen&scrollto=1

Waar moet je in ieder geval op letten als mensen zich via internet kunnen inschrijven voor de bijeenkomst?
- Zorg voor een beveiligde verbinding.
- Vraag niet meer gegevens dan noodzakelijk.
- Leg goed uit waarom u de gegevens verzamelt.
- Bewaar de gegevens niet langer dan nodig.

Wilt u de deelnemerslijst van uw evenement delen onder uw bezoekers, zodat zij bijvoorbeeld makkelijk kunnen netwerken?
Vraag dan vooraf aan de bezoekers of zij contactgegevens voor dit doel willen delen en zo ja, welke. Misschien willen zij bijvoorbeeld wel een zakelijk telefoonnummer delen, maar geen 06-nummer op de deelnemerslijst laten plaatsen. U kunt eenvoudig om toestemming vragen op het moment dat iemand zich inschrijft voor uw evenement. Die toestemming moet vrijelijk en ondubbelzinnig worden gegeven. U moet kunnen aantonen dat u toestemming heeft gekregen.

Wilt u bezoekers een nieuwsbrief over uw producten of diensten sturen?
Dat mag alleen als bezoekers vooraf duidelijk aangeven dat ze die nieuwsbrief willen ontvangen. Bijvoorbeeld door een vinkje te zetten. Ook moet u de bezoekers bij iedere nieuwsbrief de mogelijkheid bieden zich uit te schrijven.

Mag ik als organisator van een evenement foto's en filmpjes (laten) maken en publiceren waarop veel mensen staan?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/foto-en-film/beeldmateriaal#mag-ik-als-organisator-van-een-evenement-foto's-en-filmpjes-laten-maken-en-publiceren-waarop-veel-mensen-staan-7297

Hoe kan ik als organisator van een evenement mijn bezoekers om toestemming vragen om foto's en filmpjes te maken en publiceren?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/foto-en-film/beeldmateriaal#hoe-kan-ik-als-organisator-van-een-evenement-mijn-bezoekers-om-toestemming-vragen-om-foto's-en-filmpjes-te-maken-en-publiceren-7299

Waarover moet ik als organisator van een evenement mijn bezoekers informeren als ik om toestemming vraag om foto's en filmpjes te maken en publiceren?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/foto-en-film/beeldmateriaal#waarover-moet-ik-als-organisator-van-een-evenement-mijn-bezoekers-informeren-als-ik-om-toestemming-vraag-om-foto's-en-filmpjes-te-maken-en-publiceren-7300

Wat kan ik doen als organisator van een evenement als ik foto's en filmpjes wil maken en publiceren maar niet iedereen om toestemming kan vragen?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/foto-en-film/beeldmateriaal#wat-kan-ik-doen-als-organisator-van-een-evenement-als-ik-foto's-en-filmpjes-wil-maken-en-publiceren-maar-niet-iedereen-om-toestemming-kan-vragen-7301

Wat doe ik als organisator van een evenement als een bezoeker niet op de foto wil, maar wel naar mijn evenement wil komen?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/foto-en-film/beeldmateriaal#wat-doe-ik-als-organisator-van-een-evenement-als-een-bezoeker-niet-op-de-foto-wil-maar-wel-naar-mijn-evenement-wil-komen-7302

Wat doe ik als organisator van een evenement als een bezoeker zijn of haar toestemming wil intrekken?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/foto-en-film/beeldmateriaal#wat-doe-ik-als-organisator-van-een-evenement-als-een-bezoeker-zijn-of-haar-toestemming-wil-intrekken-7303

101. Klantcontact. Nieuwsbrief

Wat zegt de AP over Nieuwsbrief?
https://autoriteitpersoonsgegevens.nl/nl/privacyverklaring-aanmelden-nieuwsbrief

Hoe is de verplichte toestemming voor verzenden Nieuwsbrieven?
De verplichte toestemming voor het verzenden van 'nieuwsbrieven' per e-mail is (NL) geregeld in de Telecommunicatiewet. Je moet kunnen aantonen dat iemand toestemming heeft gegeven richting de toezichthouder de Autoriteit Consument en Markt. Vanwege de AVG moet je eveneens kunnen aantonen dat iemand toestemming heeft gegeven.
Je hebt hiervoor dus een bewijslast. Zorg er daarom voor dat je het aanvinken van een checkbox bijvoorbeeld logt, of op een andere wijze een bevestiging verzamelt van de inschrijving voor een nieuwsbrief. Sommige organisaties maken om die reden gebruik van een double opt-in: je meldt je aan, en bevestigt vervolgens deze aanmelding nogmaals door op een link te klikken in een e-mail die naar je toegestuurd is.

Mag ik nieuwsbrieven blijven versturen?
Ja, mits de ontvanger (actief) toestemming (opt-in) heeft gegeven voor het toesturen van de nieuwsbrief. Bij elke nieuwsbrief moet er steeds de mogelijkheid geboden worden om deze op te zeggen

Wat zijn de regels voor een nieuwsbrief onder de Telecommunicatiewet (NL) en AVG (EU)?
Voor een nieuwbrief gelden de volgende regels:

- Allereerst heeft je toestemming van de betrokkene nodig. Dat mag niet via een reeds aangevinkt “ja, ik wil” vakje. Dit moet via de zogenaamde opt/in methodiek met een open en vrije mogelijkheid tot aanvinken. De toestemming moet heel expliciet en specifiek juist voor deze nieuwsbrief zijn. Als je meerdere nieuwsbrieven heeft, voldoet één bepaald toestemming niet automatisch voor het toezenden van de rest.
- Zorg ervoor dat je alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat je wilt bereiken. Je hebt geen adresgegevens nodig voor het verzenden van een online nieuwsbrief en evenmin heb je bijvoorbeeld het geslacht van de ontvanger nodig. Vaak kunt je volstaan met de naam van de ontvanger en diens emailadres.
- Kortom: Verzamel niet meer dan nodig is. Bij deze regel gaat het overigens sec om het verzamelen, verwerken en gebruiken van informatie van een natuurlijk persoon. Algemene gegevens van een organisatie of instelling zijn geen persoonsgegevens; nadere gegevens van een contactpersoon binnen die organisatie of instelling zijn dat weer wel.
- In het kader van het toestemmingsproces moet je je klant aangeven wat er met de gegevens die je vraagt gaat doen. Voor een nieuwsbrief is dit veelal simpel: je hebt die gegevens nodig om de nieuwsbrief te kunnen verzenden en wellicht kun je ook aangeven hoe vaak je per jaar van plan bent dat te doen. Je kunt e.e.a. ook in uw privacy statement opnemen en in het toestemmingsproces daarnaar verwijzen.
- Vergeet vervolgens niet om in elke nieuwsbrief de mogelijkheid op te nemen om eenvoudig uit te kunnen schrijven. Deze mogelijkheid moet je bieden. En het liefste niet in een bijna onleesbare lettergrootte. De AVG verwacht volledige transparantie van je.
- Een transparantie die ook tot uitdrukking moet komen in het doel van de nieuwsbrief. Heb je een commercieel doel dan mag je je niet verschuilen achter allerlei fraaie mistige verhalen die tot doel hebben uw commerciële insteek juist te verhullen.

- Je moet volstrekt duidelijk zijn van wie de nieuwsbrief afkomstig is. Door de naam van de nieuwsbrief, je bedrijfslogo, je adresgegevens etc. en de wijze waarop men op een eenvoudige wijze met je in contact kan komen.

Wat zijn de privacy eisen voor een nieuwsbrief?
Alle klanten een nieuwsbrief sturen met daarin een aanbieding voor het nieuwste product? Een digitale nieuwsbrief versturen is de gemakkelijkste manier om contact te onderhouden met klanten. Aan het versturen van nieuwsbrieven zijn wel bepaalde eisen verbonden. De hoofdregel is dat vooraf af aan de klanten toestemming moet worden gevraagd. Dat kan heel eenvoudig door het aanvinken van een vakje waarin de klant toestemming geeft om zijn contactgegevens te gebruiken voor de nieuwsbrief. Een je moet kunnen controleren of alle klanten toestemming hebben gegeven voordat de nieuwsbrief de deur uitgaat.

102. Klantcontact. Online portal

Wat zegt de Autoriteit Persoonsgegevens over online portal?
https://autoriteitpersoonsgegevens.nl/nl/nieuws/uwv-overtreedt-wet-bij-verzuimbeheer-en-toegangsbeveiliging-werkgeversportaal

Wanneer voldoet een online portal eigenlijk aan de AVG?
Persoonsgegevens moeten op grond van de AVG passend worden beveiligd. In artikel 32 AVG staat dat iedere organisatie technische en organisatorische maatregelen moet treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Dus welke maatregelen passend zijn hangt af van de risico's voor de persoon van wie gegevens worden verwerkt. De AVG vereist ook dat bij de beoordeling van het beveiligingsniveau rekening wordt gehouden met de risico's in geval van vernietiging, verlies, wijziging of ongeoorloofde toegang tot de gegevens. Als in een portal alleen de namen van klanten staan zonder andere gegevens, dan is het risico voor de klant bij ongeoorloofde toegang tot die portal niet zo groot. Staan alle financiële gegevens van de klant daarin, dan is het risico een stuk groter en zullen hogere beveiligingsmaatregelen nodig zijn om een passend beveiligingsniveau te waarborgen.

Wanneer voldoet een online portal met gegevens over de gezondheid van werknemers eigenlijk aan de AVG?
De aanbieder én beheerder van een online portal met gegevens over de gezondheid van werknemers moet zorgen voor (minimaal) meerfactorauthenticatie. Het is aan de organisatie zelf om alle relevante factoren te betrekken in een risicoanalyse om het juiste beveiligingsniveau te bepalen.

103. Klantcontact. Visitekaartjes, E-mail, CRM-systeem

Wat zegt de Autoriteit Persoonsgegevens over visitekaartje?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/algemene-informatie-avg?qa=visitekaartje&scrollto=1

Geef je een visitekaartje af?
Een visitekaartje heb je om aan anderen te geven, zodat ze contact met je op mogen nemen. Het is dus altijd toestemming om met die persoon contact op te mogen nemen. Dat heb je nodig om te voorkomen dat je een spammer bent. Voor spam hebben we de Telecommunicatiewet die in 2019 vervangen gaat worden door de ePrivacyverordening. De AVG gaat alleen over het mogen verwerken van de persoonsgegevens.

Krijg je een visitekaartje?
Dan mag je die ook opnemen in je adressenbestand. Je mag deze persoon alleen nog niet zomaar nieuwsbrieven of andere commerciële berichten toesturen. Deze mensen moeten wel kunnen weten wat je met hun gegevens doet. Beetje lastig om alle informatie met ze te delen als je dat visitekaartje ontvangt. Zorg daarom dat je die informatie wel beschikbaar maakt via een privacyverklaring die je bij het eerste mailcontact kunt toesturen of waar je met een link naar kunt verwijzen.

Wat zijn de regels voor emails?
Als je een e-mail stuurt naar een potentiële opdrachtgever op een info@e-mailadres dan heb je geen toestemming nodig, maar voor een e-mail naar persoonsnaam@website.nl dan heb je een expliciete opt-in toestemming nodig. Je moet kunnen bewijzen dat je deze toestemming hebt verkregen en hoe deze is verkregen. De impliciete toestemming (soft opt-in) waarbij je alleen de mogelijkheid van opt-out biedt is niet langer toegestaan.

Wat is toegestaan voor een CRM-systeem?
Het uploaden van deelnemerslijsten van bijvoorbeeld events in de marketingdatabase of CRM-systeem is niet meer toegestaan zonder expliciete opt-in, evenals het gebruik van ingekochte bestanden met leads. Ook deze dienen opt-in compliant te zijn. Zelfs de persoonlijke contacten van salesmedewerkers kunnen niet zomaar toegevoegd worden aan het CRM-systeem. Ook hiervoor dien je te kunnen aantonen wanneer en hoe er toestemming is verleend. Tenslotte ben je verplicht om te checken of alle partijen waarmee je gegevens uitwisselt ook AVG compliant zijn voor hun dataverzameling.

104. Klantcontact. Webwinkel/ webshop

Wat zegt de Autoriteit Persoonsgegevens over een Webwinkel?
https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/register-zwarte-lijsten/zwarte-lijst-detailhandel

Wat zegt de ACM over een Webwinkel?
- https://www.acm.nl/nl/onderwerpen/verkoop-aan-consumenten/verkopen-aan-consumenten/checklist-verkoop-via-internet
- https://www.acm.nl/sites/default/files/documents/2017-12/Checklist-verkoop-via-internet_0.pdf

Over welke persoonsgegevens moet een webwinkel de bezoeker informeren?
Een webwinkel is verplicht klanten en bezoekers te informeren over welke privacygevoelige informatie de webwinkel verzamelt en met welk doel. Ook als dat doel alleen maar is het vastleggen van hun gegevens in een klantenbestand. Wanneer een webwinkel van de klant een profiel opbouwt om gedrag of interesses te kunnen voorspellen, moet zij de klant hierover duidelijk informeren.

Hoe informeert de webwinkel de bezoeker over privacy?
Informeren kan via een (online) privacyverklaring. Bezoekers en klanten moeten die eenvoudig kunnen vinden op de website en de informatie in de verklaring moet duidelijk en gemakkelijk leesbaar zijn. Als de webwinkel ook cookies plaatst of laat plaatsen, moet zij haar bezoekers ook informeren over deze cookies. In de meeste gevallen moet zelfs voordat cookies mogen worden geplaatst, door een bezoeker toestemming worden gegeven.

Hoe voldoet de MAAS webwinkel aan het AVG recht van bezwaar?
Als website- of webshophouder dien je de klant te informeren dat hij of zij bezwaar kan maken tegen het verdere gebruik van zijn of haar gegevens voor marketingdoeleinden. Hier moet je altijd gehoor aan geven, tenzij je gerechtvaardigde argumenten hebt die zwaarder wegen dan die van de klant.

Hoe voldoet de MAAS webwinkel aan de AVG informatieverplichting
Als website- of webshophouder heeft MAAS de taak om bij klanten duidelijk aan te geven wat er met hun gegevens gedaan wordt. Dit is aangegeven in de MAAS privacyverklaring.

Hoe is de MAAS webwinkel beveiligd?
De webwinkel heeft passende technische en organisatorische beveiligingsmaatregelen om misbruik en ongeautoriseerde toegang tot deze gegevens tegen te gaan. De SSL(TLS)-verbinding voor een webwinkel verplicht.

Wat is SSL?
SSL is een afkorting voor Secure Socket Layer. SSL is een manier voor het creëren van een beveiligde verbinding tussen een webserver en een internetbrowser. Deze verbinding verzekert dat alle gegevens, die tussen de webserver en browser worden verstuurd, geheim blijven voor buitenstaanders en niet gestolen kunnen worden. Pagina's waar een zogenaamd 'slotje' zichtbaar is in de adresbalk is een kenmerk van SSL.

Hoe dien je Google Analytics te gebruiken?
Zie de Handleiding privacyvriendelijk instellen van Google Analytic van de AP:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleiding_privacyvriendelijk_instellen_google_analytics.pdf

Gebruik Google Analytics niet toegestaan?
De Oostenrijkse privacytoezichthouder rondde in januari 2022 een onderzoek af naar het gebruik van Google Analytics door een Oostenrijkse website. Google Analytics blijkt volgens de Oostenrijkse toezichthouder in dit onderzochte geval niet aan de Algemene verordening gegevensbescherming (AVG) te voldoen.
De AP onderzoekt sinds 13 januari 2022 twee klachten over het gebruik van Google Analytics in Nederland afronding van dat onderzoek begin 2022, kan de AP zeggen of Google Analytics nu is toegestaan of niet.

Aanbeveling Functionaris Gegevensbescherming
Zorg voor:
- opt in
- bewijslast (logging) van de toestemming.

Welke NL (EU) regels gelden voor business-to-business (B2B)?
Als u verkoopt aan andere bedrijven, stichtingen en verenigingen (business to business, B2B) dan vallen deze klanten niet onder het consumentenrecht. Dat betekent onder meer dat:
- uw klanten geen wettelijke bedenktijd hebben (u mag wel bedenktijd geven, dit zet u in de algemene voorwaarden)
- er minder garantieregels gelden dan voor consumenten (u zet de beperkte garantie in de algemene voorwaarden)

Bij B2B gelden de algemene regels voor (koop)overeenkomsten uit boek 6 en boek 7 van het Burgerlijk Wetboek.
https://ondernemersplein.kvk.nl/regels-voor-online-verkoop/

Alle klanten een nieuwsbrief sturen met daarin een aanbieding voor het nieuwste product? Een digitale nieuwsbrief versturen is de gemakkelijkste manier om contact te onderhouden met klanten. Aan het versturen van nieuwsbrieven zijn wel bepaalde eisen verbonden. De hoofdregel is dat vooraf af aan de klanten toestemming moet worden gevraagd. Dat kan heel eenvoudig door het aanvinken van een vakje waarin de klant toestemming geeft om zijn contactgegevens te gebruiken voor de nieuwsbrief. Een je moet kunnen controleren of alle klanten toestemming hebben gegeven voordat de nieuwsbrief de deur uitgaat.

105. Inspecties. Rijksoverheid

Waar vind ik de verwerkingsregisters van de inspecties rijksoverheid?
https://www.avgregisterrijksoverheid.nl/

Onder welk ministerie valt de Nederlandse Voedsel en Waren Autoriteit (NVWA) en welke privacy regels gelden voor de NVWA?
De Nederlandse Voedsel- en Warenautoriteit (NVWA) maakt deel uit van het ministerie van Landbouw, Natuur en Voedselkwaliteit (LNV). De NVWA gaat zorgvuldig om met uw persoonsgegevens. De bescherming van deze gegevens is geregeld in de Algemene verordening gegevensbescherming (AVG) en de Wet politiegegevens (Wpg). De AVG en de Wpg hebben tot doel de privacy van burgers te beschermen. Je deelt persoonsgegevens met de NVWA als je contact opneemt, bijvoorbeeld als je een vraag stelt. De NVWA vraagt ook om persoonsgegevens in verband met haar publiekrechtelijke en wettelijke taken. Voorbeelden van persoonsgegevens zijn naam, telefoonnummer of e-mailadres. Maar ook het IP-adres van een computer of Burgerservicenummer. Het gaat om alle gegevens die we in verband kunnen brengen met u. Wanneer uw persoonsgegevens worden verwerkt vanwege strafrechtelijke handhaving worden die persoonsgegevens 'politiegegevens' genoemd.

Onder welk ministerie valt de Inspectie Leefomgeving en Transport (ILT) en welke privacy regels gelden voor de ILT?
Het ministerie van Infrastructuur en Waterstaat heeft een functionaris voor gegevensbescherming (FG) die ook de wettelijke taken uitvoert voor de ILT. De bescherming van deze gegevens is geregeld in de Algemene verordening gegevensbescherming (AVG) en de Wet politiegegevens (Wpg).

Onder welk ministerie valt de Inspectie Sociale Zaken en Werkgelegenheid (SZW) en welke privacy regels gelden voor de SZW?
De SZW-inspectie maakt deel uit van het ministerie van Ministerie van Sociale Zaken en Werkgelegenheid. De Inspectie SZW mag voor het uitvoeren van haar wettelijke taak persoonsgegevens opvragen én ontvangen. Dit is geregeld in artikel 6, eerste lid, onder c van de AVG. Dit betekent dat, naast gegevens die MAAS zelf aanlevert, bijvoorbeeld ook een werkgever of een ander bestuursorgaan gegevens kan leveren aan de Inspectie SZW zonder de AVG of de Wpg te overtreden.

Welke regels gelden bij inspectie SZW van een thuiswerkplek?
De Inspectie SZW controleert bedrijven op de naleving van de Arbeidsomstandighedenwet (Arbowet). Daarvoor moeten inspecteurs toegang hebben tot het pand, de werkplek en alle andere plaatsen die de inspecteur wil onderzoeken. Dat kan ook de thuiswerkplek zijn.
Op grond van de Arbowet mag de inspecteur de woning van een thuiswerker bekijken, ook als de bewoner daar geen toestemming voor geeft. Aan de andere kant is een woning ook privéruimte. Daarom geldt een aantal regels:

1. De inspecteur moet altijd eerst toestemming vragen.
2. Geeft de werknemer geen toestemming, dan mag de inspecteur de woning pas betreden als hij hier een schriftelijke machtiging voor heeft.
3. De inspecteur moet zich vooraf legitimeren.
4. De inspecteur moet de werknemer ruim op tijd inlichten over zijn bezoek. Samen maken ze een afspraak over de datum en het tijdstip van het bezoek.
5. De inspecteur mag niet alleen komen. Er moet altijd een tweede inspecteur bij zijn.
6. De werknemer mag vragen om de aanwezigheid van minstens één vrouwelijke inspecteur.

7. Verplichtingen van inspecteur liggen vast in gedragscode.

Welk omgevingsdienst verwerkt de persoonsgegevens bij zaken rond het Omgevingsrecht voor hoofdkantoor MAAS?
Dat is de Omgevingsdienst Zuidoost-Brabant. Het Ministerie van Economische Zaken en Klimaat vraagt van bedrijven om zelf te melden wat ze aan energiebesparingsmaatregelen nemen. Omgevingsdiensten en gemeenten moeten dat controleren. Gemeenten, provincies, de waterschappen een aantal uitvoerende taken op het gebied van Bouwen, Ruimte en Milieu onder in Omgevingsdiensten of Regionale uitvoeringsdiensten (RUD's).
ODZOB verwerkt alleen persoonsgegevens, als hiervoor een rechtmatige grondslag aanwezig is. Denk hierbij aan de uitvoering van een wettelijke verplichting, het vitale belang van u als betrokkene of wanneer de verwerking noodzakelijk is voor de vervulling van een taak in algemeen belang.

106. Inspecties. Zelfstandige bestuursorganen (ZBO) en voluntary standards

Wat zegt de Autoriteit Persoonsgegevens over een ZBO?
Geen specifieke informatie

Wat is het privacy beleid van de biologische inspectie (SKAL)?
https://www.skal.nl/over-ons/privacy/
Persoonsgegevens worden in beginsel alleen gebruikt door Skal en de volgens de relevante wet- en regelgeving betrokken partijen die in het kader van de inspectie van toepassing zijn. Skal verstrekt persoonsgegevens niet aan derden zonder toestemming, tenzij Skal daartoe verplicht is op basis van de wet of een rechterlijke uitspraak of als dit noodzakelijk is voor de uitvoering van een overeenkomst tussen MAAS en Skal.

Wat is het privacy beleid van de fairtrade inspectie (FLOCERT)?
https://www.flocert.net/privacy-policy/
Grondslag voor verwerking van persoonsgegevens door FLOCERT is toestemming: *The legal basis for data processing is the 1st sentence of point (f) of Art. 6(1) GDPR.*

Wat is het privacy beleid van de externe audit voor de ISO- en PSO-certificatie (DNV GL)?
https://www.dnvgl.nl/privacy/index.html
Grondslag voor verwerking persoonsgegevens is door DNV GL is toestemming: *The legal basis for data processing is the 1st sentence of point (f) of Art. 6(1) GDPR.*

107. Fleetmanagement - Ritregistratie

Wat zegt de Autoriteit Persoonsgegevens over controle van personeel:
https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-uitkering/controle-van-personeel

Is een privacy regeling Persoonsgegevens rittenadministratie noodzakelijk?
Rittenadministratie met behulp van een rittenregistratiesysteem legt persoonsgegevens vast, zoals de locatie waar de auto is, het kenteken van de auto en het aantal privékilometers. De werknemer heeft een aantal rechten met betrekking tot die gegevens. De werkgever moet de werknemer bijvoorbeeld niet alleen informeren over welke gegevens er verzameld worden, maar ook wie die data kan inzien en voor welke doeleinden de data gebruikt worden. Die informatie hoort in de MAAS autoregeling of in een apart document. Bijgevoegd: Stramien voor Privacyregeling Ritregistratiesysteem op basis van de Gedragscode Ritregistratiesysteem “Gedragscode Privacy RRS”

Is voor rittenregistratie (regeling) instemming van de Ondernemingsraad vereist?
Voor het invoeren van een rittenregistratie- of Track en Trace systeem is instemming vereist van de ondernemingsraad. Als die er namelijk niet is, moeten er afspraken gemaakt worden met individuele werknemers. Deze vragen moeten beantwoord en vastgelegd worden:

- Is er een noodzaak? Omdat de positie van de auto’s middels deze module grafisch inzichtelijk zijn kunnen we de planning van monteurs optimaliseren.
- Wat doet MAAS met de gegevens? RAM heeft een standaard interface pakket waardoor we nu een voorschot kunnen nemen op automatisch plannen. We kunnen de urenregistratie van monteurs gaan automatiseren, dit gebeurt nu nog handmatig in Excel.
- Is de privacy van werknemers gewaarborgd? Voor de berijders die bijtelling betalen is de auto voorzien van een Privé/Zakelijk knop die de positie bepaling uitschakelt en alleen de gereden kilometers bijhoudt.
- Worden privékilometers volledig afgeschermd? …
- Kan de werknemer de verzamelde gegevens inzien? De medewerker krijgt wekelijks inzicht in de gereden kilometers van de week ervoor ter controle.
- Kan de werknemer de gegevens gebruiken voor diens kilometeradministratie? Het systeem is aangesloten om de Canbus van de auto waardoor altijd de kilometerstand van de auto zelf wordt bijgehouden en dus wordt de kilometerregistratie geautomatiseerd.
- Wie kunnen er bij de gegevens en hoe wordt dit beschermd en gewaarborgd? …

Heeft ritregistratiesysteem Track-and-trace Fiscaal van RAM Mobile Data het keurmerk RSS?
Ja, RAM voldoet aan strenge vereisten op verschillende domeinen als veiligheid, continuïteit en fiscaliteit, zoals uitgeschreven door de Stichting Keurmerk RitRegistratieSystemen (RSS).

Wie is verantwoordelijk voor de registratie van het karakter van een rit?
De berijder is zelf verantwoordelijk voor de juiste bepaling en registratie van het karakter van de rit.

Is een gecertificeerd ritregistratiesysteem wettelijk verplicht?
Nee, voor het leveren van bewijs in het kader van de bijtellingsregeling privégebruik auto geldt de vrije bewijsleer. Het bewijs wordt in de regel geleverd in de vorm van een sluitende ritregistratie (handmatig of geautomatiseerd). Omdat bij een gecertificeerd ritregistratiesysteem geen mogelijkheid bestaat om oorspronkelijke ritgegevens te verwijderen kan met zo'n systeem worden volstaan met een andere vorm van toezicht (controle op volledigheid is in beginsel overbodig, behalve daar waar sprake is van gemelde verstoringen). De Belastingdienst houdt bij de uitvoering

van haar handhavende en toezichthoudende taken zo goed mogelijk rekening met de kwaliteitswaarborgen en beheersingsmaatregelen in de administratieve keten. Daarom houdt zij ook rekening met de bijdrage die een keurmerk daaraan levert.

Van wie is het Keurmerk RRS?
Het keurmerk is niet van de Belastingdienst maar van de markt. De keurmerkorganisatie maakt onderdeel uit van het Electronic Commerce Platform Nederland (ECP). Dat is een publiek-, private samenwerking tussen bedrijven, overheid en maatschappelijk organisaties en heeft tot doel het gebruik van ICT in de Nederlandse samenleving te versterken door onder meer de digitale veiligheid te verbeteren. De Belastingdienst is betrokken bij de normen en eisen welke het keurmerk stelt aan de te certificeren systemen. Het keurmerk RRS wordt afgegeven door een onafhankelijke stichting (Stichting Keurmerk RitRegistratieSystemen). De uitgifte van het keurmerk is gebaseerd op het oordeel van een externe auditor.

Wat wordt verstaan onder een “nagenoeg gelijkwaardig” systeem?
SKRRS ziet een systeem als “nagenoeg gelijkwaardig” (aan een systeem waarop een Keurmerk is afgegeven) indien het systeem naast een systeem met een Keurmerk wordt geleverd en de volgende kenmerken heeft: Het systeem heeft dezelfde configuratie van hardware & software. Het systeem wordt geleverd in Nederland. Het systeem is gekoppeld aan een voertuig met chauffeur. Het systeem is gekoppeld aan een voertuig dat is voorzien van een kenteken voor voertuigen onder 3.500 kg (WAM-plichtig).

108. Fleetmanagement - Verkeersboete

Wat zegt de Autoriteit Persoonsgegevens over verkeersboete verwerking:
Geen info.

Wat zegt de Autoriteit Persoonsgegevens over verkeersboete verwerking:
https://www.cjib.nl/verkeersboete-en-verwerking-van-persoonsgegevens

Wat zegt de jurist over verkeersboete verwerking:

- https://www.dirkzwager.nl/kennis/artikelen/hvjeu-gegevens-over-verkeersovertredingen-privacygevoelig-wetgeving-opvragen-strafpunten-ongeldig/
- https://bz.nl/wp-content/uploads/2023/02/NTB-2022-115-AVG-Kroniek-gedrukt.pdf

Mogen toegekende punten op een puntenrijbewijs zomaar worden verwerkt?
Toegekende punten op een puntenrijbewijs mogen niet zomaar worden verwerkt. Deze gegevens vallen onder de extra strenge regels inzake strafrechtelijke gegevens. Wat strafrechtelijke gegevens zijn moet in de hele Europese Unie op dezelfde manier worden geïnterpreteerd. Letse wetgeving die het mogelijk maakte om de aan iemand toegekende punten op te vragen is in strijd met die strenge regels. Dit alles volgt uit een recente beslissing van het Hof van Justitie. Deze beslissing heeft ook gevolgen voor Nederland.
Toegekende punten op een puntenrijbewijs mogen niet zomaar worden verwerkt. Deze gegevens vallen onder de extra strenge regels inzake strafrechtelijke gegevens. Wat strafrechtelijke gegevens zijn moet in de hele Europese Unie op dezelfde manier worden geïnterpreteerd. Letse wetgeving die het mogelijk maakte om de aan iemand toegekende punten op te vragen is in strijd met die strenge regels. Dit alles volgt uit een recente beslissing van het Hof van Justitie. Deze beslissing heeft ook gevolgen voor Nederland.
Aanleiding: kritiek op delen van strafpunten. De situatie die heeft geleid tot de uitspraak is overzichtelijk. Aan persoon B zijn strafpunten toegekend wegens verkeersovertredingen. Deze strafpunten staan aangetekend in het nationale Letse register van voertuigen en bestuurders. Aangezien in Letland dit register openbaar is, heeft iedereen deze gegevens kunnen opvragen. Persoon B stelt dat een dergelijk systeem zijn privacy schendt en start daarop een procedure voor de rechtbank in Letland.
Letse instanties overtuigd, alleen privacy toezichthouder twijfelt. In de procedure in Letland worden zowel het Letse Parlement, de directie verkeersveiligheid en de Letse privacy toezichthouder gehoord. Het Letse parlement benadrukt dat het inderdaad de bedoeling is dat de gegevens vrij opgevraagd kunnen worden nu dit de verkeersveiligheid zou verbeteren en het ook aansluit bij het grondwettelijke recht op toegang tot informatie. De directie verkeersveiligheid benadrukt dat de wet geen beperkingen stelt aan het gebruik van de informatie. Er zijn contracten met commerciële aanbieders gesloten waarin is vastgelegd dat deze aanbieders niet meer informatie mogen tonen dan de informatie die is verkregen uit het register. Net als bij het parlement lijkt absoluut geen sprake van twijfel of het systeem als zodanig rechtmatig is. De privacytoezichthouder geeft wel aan te twijfelen of de noodzaak voor het systeem wel is aangetoond en of het systeem wel proportioneel is.
Letse rechter stelt vragen. De Letse rechter vraagt zich af of het systeem van openbaarmaking van de punten wel is te verenigen met de AVG. De rechter vraagt dan ook aan het Hof van Justitie uitleg over de AVG. Meer specifiek vraagt de rechter zich onder meer af of de verstrekking van de gegevens niet haaks staat op het verbod in de AVG op de verwerking van strafrechtelijke gegevens en of de wetgeving die dit toestaat niet in strijd is met beginselen uit de AVG.

Om welke gegevens gaat het in Letland?
Het is wat zoeken in de uitspraak om welke gegevens het nu precies gaat. Gelet op wat onder meer in overweging 42 en 43 staat vermeld vermoed ik echter dat zowel de overtreding als het daarvoor toegekende aantal punten in het register worden vermeld (en ik vermoed op grond van logica ook een veld als datum).

Welke AVG jurisprudentie in Letland?
Hof: AVG is van toepassing. Het Hof moet eerst de vraag beantwoorden of de AVG wel speelt. Daar is het Hof echter snel klaar mee: het verstrekken van gegevens over de punten is een verwerking van persoonsgegevens. Bovendien zijn de uitzonderingen uit de AVG niet van toepassing: de meeste uitzonderingen moeten heel strikt worden geïnterpreteerd. De enige uitzondering met enig raakvlak gaat over de verwerking in het kader van opsporing en vervolging en juist dat speelt niet bij openbaarmaking van dit soort gegevens. De AVG is dus 'gewoon' van kracht. Hof: bescherming strafrechtelijke gegevens dient hoog doel. Vervolgens benadrukt het Hof het belang van het verbod op het verwerken van strafrechtelijke gegevens. Het hof spreekt over gegevens met een "bijzondere gevoeligheid" die "in zeer ernstige mate inbreuk kunnen maken" op grondrechten. Strafrechtelijke gegevens kunnen namelijk "aanleiding geven tot maatschappelijke afkeuring, zodat het feit dat toegang wordt verleend tot dergelijke gegevens de betrokkene kan stigmatiseren en aldus op ernstige wijze inbreuk kan maken op zijn privé- of beroepsleven." Hof: Europees uitleggen wat strafrechtelijke gegevens zijn Het Hof benadrukt dat begrippen uit de AVG, tenzij naar nationaal recht wordt verwezen, in beginsel in de hele Unie autonoom en uniform moeten worden uitgelegd (r/o 81). Het moet niet zo zijn dat de bescherming die de AVG biedt van land tot land verschilt omdat er verschillend naar verkeersovertredingen wordt gekeken (r/o 83).
Het Hof geeft drie criteria om te beoordelen of een strafbaar feit van strafrechtelijke aard is. Daarbij geeft het Hof ook direct wat kanttekeningen, die ik in onderstaand schema direct verwerk:

1. juridische kwalificatie naar nationaal recht; kanttekening 1: die kwalificatie is niet doorslaggevend (immers: Europees uniform interpreteren, zie r/o 80-82); kanttekening 2: zelfs feiten die naar nationaal recht niet strafrechtelijk van aard zijn, kunnen dat in EU-verband wel zijn (zie r/o 88);
2. aard van het strafbare feit: de sanctie moet een repressief doel dienen (eventueel ook preventief), doch niet louter reparatoir (zie r/o 89);
3. zwaarte van de sanctie; opmerking: het Hof is niet heel helder wat "zwaar genoeg" is, maar alles overwegend lijkt dit een lage drempel, zeker ook gelet op de verwijzing naar het EHRM dat in beginsel verkeersovertredingen als strafrechtelijk ziet.

Vervolgens concludeert het Hof dat gegevens over verkeersovertredingen die kunnen leiden tot toekennen van strafrechten in ieder geval vallen onder het verbod van artikel 10 AVG (r/o 93). In het dictum formuleert het Hof het zelfs nog iets ruimer, door te bepalen dat artikel 10 AVG "van toepassing is op de verwerking van persoonsgegevens die betrekking hebben op strafpunten die aan bestuurders van voertuigen zijn toegekend wegens verkeersovertredingen".
De verwerking van gegevens over de strafpunten valt dus onder het verbod uit de AVG. Daarmee is de kwestie echter nog niet af, want de AVG bepaalt dat nationale wetgeving de verwerking toch kan toestaan.
Hof: AVG biedt ruimte voor nationale regelingen, mits ze voldoen aan de AVG
Het Hof van Justitie komt daarop toe aan het onderzoeken van de Letse wetgeving. De Letse rechter had daarover een vrij specifieke vraag gesteld, maar het Hof leest daarin de bredere vraag of die wetgeving wel te verenigen is met de AVG (r/o 97).
Het Hof benadrukt daarop dat iedere verwerking moet voldoen aan de beginselen die vastliggen in artikel 5 en 6 AVG (r/o 97). Het Hof benadrukt echter ook dat de AVG aan nationale lidstaten ook veel ruimte laat, nu diezelfde beginselen geen harde verboden kennen (r/o 103-104). Sterker nog, privacy is niet absoluut en moet worden afgewogen tegen andere grondrechten (r/o 105). Wel is het

zo dat inbreuken op de privacy moeten voldoen aan strikte eisen van noodzakelijkheid en voorzienbaarheid (r/o 105). Daarbij moet ook worden getoetst op proportionaliteit, subsidiariteit en evenredigheid (r/o 106).
Daarop komt het Hof aan de meer inhoudelijke toets. Het Hof stelt vast dat het verbeteren van de verkeersveiligheid op zichzelf een door de Unie erkend doel is (r/o 108). Dat doel moet dan echter wel op de meest privacyvriendelijke wijze worden nagestreefd (r/o 109-110). In andere lidstaten worden hele andere maatregelen getroffen en Letland lijkt die andere routes niet eens onderzocht te hebben (r/o 111). Bovendien blijkt nergens uit dat het ingevoerde systeem werkt (r/o 116). Dat hiermee notoire overtreders beter in beeld komen kan onder omstandigheden zinvol zijn, maar rechtvaardigt nog niet de openbaarmaking van hun gegevens (r/o 114). Bovendien maakt het systeem ook helemaal geen onderscheid tussen gewone en notoire overtreders (r/o 115). Dit terwijl de gegevens de bestuurders ernstig kunnen stigmatiseren (r/o 112-113).
De nationale wet voldoet dus niet aan de basisprincipes van de AVG. Het verstrekken van de gegevens is dus niet toegestaan.

Wat is de vertaling naar Nederland?
In Nederland zijn gegevens over verkeersovertredingen niet op te vragen door het publiek. In die zin is het arrest niet direct op onze praktijk toepasbaar. Er zitten echter genoeg interessante aspecten aan het arrest die maken dat ik het toch behandel.
Het Hof geeft een ruime, beste laagdrempelige uitleg, aan het begrip strafrechtelijke persoonsgegevens. Toegekende strafpunten, althans de daaraan ten grondslag liggende gegevens over overtredingen, vallen hier (al) onder.
Die grens ligt dus (veel) lager dan tot op heden in Nederlands rechtspraak werd aangenomen. Naar Nederlands recht werd immers onder strafrechtelijke gegevens veelal verstaan “zodanig concrete feiten en omstandigheden dat zij een als strafbaar feit te kwalificeren bewezenverklaring (…) kunnen dragen.”. Een enkele aangifte of iets dergelijks was hiervoor onvoldoende.
Ik vraag me af of dit Nederlandse kader dus houdbaar is. De huidige uitspraak laat immers zien dat het enkele feit dat een delict is begaan waarop een strafpunt staat al onder het begrip valt. De hoge drempel van voldoende feiten en omstandigheden om te kunnen komen tot een bewezenverklaring wordt niet gesteld (=o.a. meerdere bewijsmiddelen, voldoen aan alle delictbestanddelen, etc.). Wel lijkt bij het HvJEU het mogelijke gevolg voor de betrokkene zwaar te wegen (en daarvoor de aard van het delict althans de kans op stigmatisering weer mee te wegen).
Dit roept de vraag op hoe om te gaan met bijvoorbeeld iets ogenschijnlijk simpels als het vastleggen van de bewering van een klant dat hij/zij krap bij kas zit vanwege het betalen van veel boetes. Of denk aan het verhalen van verkeersboetes op leaserijders. Het lijkt verstandig in ieder geval niet vast te leggen wat de achtergrond van die boetes was.
Opmerkelijk is overigens verder dat Nederland een eigen draai geeft aan het begrip strafrechtelijke persoonsgegevens. Volgens de UAVG vallen hier niet alleen de gegevens als bedoeld in artikel 10 AVG onder, maar ook de “persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag” (zie artikel 1 UAVG). Ook dit lijkt lastig vol te houden gelet op de uniforme uitleg die het HvJEU aan het begrip geeft (in samenhang met het beginsel van vrije uitwisseling van gegevens binnen de EU).
Een ander aspect dat opvalt aan deze zaak is de directe toetsing van de nationale wetgeving aan de beginselen uit de AVG. Dit is nog niet zo vaak voorgekomen. Het HvJEU legt de lat echter hoog; de eisen die aan nationale wetgeving worden gesteld die zien op de verwerking van persoonsgegevens zijn streng. Tegelijkertijd is ook fraai om te zien dat het Hof het beginselkarakter van de AVG benadrukt: binnen de kaders die de beginselen stellen is er veel ruimte voor lidstaten om te komen tot een eigen invulling met eigen wetgeving. Het ligt wel voor de hand dat het Hof dit laatste steeds strikter en "Europeser" gaat interpreteren (zoals we het EHRM ook op thema's hebben zien doen

door de decennia heen), vermoedelijk met uitzondering van (althans meer terughoudendheid bij) die bepalingen in de AVG waar expliciet ruimte wordt gelaten aan nationale wetgeving.

109. AVG en Afdeling Planning & Control

Wat zegt de Autoriteit Persoonsgegevens over P&C?
Geen specifieke informatie

Wat betekent AVG voor dagelijkse werkzaamheden binnen Planning & Control?

Wat zijn persoonsgegevens?
Persoonsgegevens zijn alle gegevens die naar een bepaalde persoon kunnen linken. Naam, adres telefoonnummer etc. Maar ook godsdienst, huidskleur, foto's en dergelijke.

Onbewust de fout in gaan?
Bij veel dagelijkse werkzaamheden staan we niet stil dat we persoonsgegevens verspreiden. Denk bijvoorbeeld aan bestanden (Excel/word) mailen waar persoonsgegevens in staan of foto's van een activiteit plaatsen op internet.
Denk na vooral bij wat je doet, dit is al het halve werk!
Als je bestanden mailt denk dan na of het noodzakelijk is dat alle persoonsgegevens gedeeld worden, kun je met minder gegevens ook het werk doen? Zet alleen diegene in de mail die de gegevens moeten ontvangen? Stel eventueel een wachtwoord in om het bestand te kunnen openen zodat de gegevens beveiligd zijn.

Wat doe ik als een klant of operator vragen stelt over AVG?
Aangezien wij op de afdeling veel klant/operator contact hebben kan het zijn dat je vragen krijgt over AVG. Ga nooit zelf in op deze vragen. Laat de klant/operator zijn vragen mailen naar fg@maas.nl Of verbind degene door met de FG.

Mag ik een naam en telefoonnummer noteren van een klant?
Een naam kun je wel noteren bij een storingsmelding. Ben met een telefoonnummer voorzichtig. Ga hierbij na, is het nummer noodzakelijk? Wil de klant een product na gebracht krijgen dan kun je het telefoonnummer noteren bij de melding in SAP. Je hebt immers een doel met de gegevens, namelijk de klant compenseren.
Heb je het telefoonnummer nodig om bijvoorbeeld een klant terug te bellen, dat kan. Je 'doel' is service verlenen aan de klant. Om dit uit te kunnen voeren heb je zijn telefoonnummer nodig. Je mag de telefoonnummers niet bewaren dus sla het nummer na gebruik niet op, delete het of gooi het briefje weg.
TIP: Je kunt ook een telefoonnummer van het bedrijf noteren, dit is geen privénummer, niet gerelateerd aan een persoon.

Mag je nog geld terug geven op de bankrekening van een klant?
Ja, dat mag. De klant geeft je zelf zijn gegevens, je hebt hier niet om gevraagd dus dat mag.
Je slaat de gegevens op in een Excel bestand. Dit bestand mag je niet lang bewaren, want hierin staan persoonsgegevens zoals een bankrekeningnummer en hier voor geldt een bewaartermijn. Je moet de opgeslagen bestanden van voorgaande maanden wissen na xx maanden.

Werken in Portals van diverse bedrijven?
Hou er rekening mee dat alle informatie die je doorgeeft in een portal van PostNL, ING, Gemeente Rotterdam etc. in principe gegevens doorgeven is aan derde. Dit mag niet zomaar. Zet in de melding bijvoorbeeld 'de operator' in plaats van een naam of geef een bedrijfstelefoonnummer door.

Kan ik post versturen naar operators?
Ja dat kan.

Mag ik medewerkers aanmelden bij de klant?
Een naam kan je doorgeven aan de klant. Verder mag je niet zomaar gegevens doorgeven aan de klant, dit is gegevens doorgeven aan derden en hier gelden regels voor. De klant moet zich ook aan de wet houden en moet MAAS aangeven waarom hij bepaalde gegevens nodig. Wat is zijn doel? Ga niet zelf bij de klant navraag doen, overleg met je leidinggevende of met de AVG functionaris.

Het gaat niet goed, wat doe ik?
Zie je dat er ergens gegevens worden verwerkt of verspreid die niet aan de nieuwe wet voldoen geef het dan door! We moeten allemaal wennen aan de nieuwe wet en verspreiden vaak onbewust verkeerd de gegevens. Door het te melden kunnen we het verbeteren en er samen voor zorgen dat Planning & Control klaar is voor de nieuwe AVG wet!

Onduidelijkheden, vragen?
Staat je vraag er niet tussen, laat het weten!

110. G&VW. Alcohol & drugs

Wat zegt de AP over persoonsgegevens en controles op het gebruik van alcohol, drugs en geneesmiddelen in de arbeidsrelatie:

- https://autoriteitpersoonsgegevens.nl/nl/nieuws/testen-op-alcohol-drugs-geneesmiddelen-tijdens-werktijd-alleen-met-wettelijke-regeling
- https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/informatieblad_testen_op_alcohol_drugs_en_geneesmiddelen_def.pdf

Verdere perventie info?
https://www.drugsenuitgaan.nl/hulp-en-advies/veel-gestelde-vragen

Welke eisen aan beleid op het gebied van alcohol, drugs en geneesmiddelen in de arbeidsrelatie?
Bij beleid op het gebied van alcohol-, drugs- en medicijngebruik gaat het om bijzondere persoonsgegevens. Dergelijk beleid moet gericht zijn op preventie en begeleiding; de bijbehorende procedure mag geen sancties bevatten. Check uw beleid en pas het zo nodig aan (of laat dit doen). Het is ook verstandig om de afspraken met uw arbodienst op dit punt nog eens na te lopen.

Wanneer mag werkgever testen op drugs en alcohol?
Het tijdens werktijd testen van werknemers op alcohol, drugs en geneesmiddelen is alleen toegestaan als er voor een bepaald beroep specifieke wetgeving geldt. In de meeste gevallen is het verboden, zo laat de Autoriteit Persoonsgegevens (AP) weten.
Het afnemen van een drugstest is overigens aan veel regels gebonden. Een Nederlandse werkgever kan je dan ook niet zomaar verplichten om een drugstest te doen. Dit mag alleen als je voor je werk bijvoorbeeld een voertuig bestuurt of gevaarlijke machines bedient. Of als je voor Defensie of bij de politie werkt. Zomaar een test uitvoeren is een inbreuk op de privacy en dat mag niet. De Autoriteit Persoonsgegevens (AP) houdt hier toezicht op. Maar met name Amerikaanse bedrijven met een Nederlandse vestiging maken zich hier wel schuldig aan, in de Verenigde Staten is er minder strenge wetgeving.

Wat heeft werkgever te zeggen over drugsgebruik in vrije tijd?
Je mag op grond van het Europese Verdrag voor de Rechten van de Mens zelf bepalen hoe je privéleven eruitziet. Drugsgebruik wordt in Nederland gezien als een privézaak. Het kan op zichzelf nooit een reden zijn voor ontslag. Maar dat verandert als het privégedrag invloed krijgt op het werk. En voor mensen met een voorbeeldfunctie of voor werknemers in de zorg, zeker als zij werken met verslaafden, zijn er wel strenge regels en kan dit dus leiden tot ontslag. De kantonrechter beslist uiteindelijk of het ontslag rechtmatig is.

111. G&VW. Arbeidsongeval melden

Wat zegt de Autoriteit Persoonsgegevens over een Arbeidsongeval?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-en-uitkering/mijn-zieke-werknemer?qa=arbeidsongeval&scrollto=1

Wat is de relevante wetgeving?
https://wetten.overheid.nl/BWBR0010346/2023-06-20#Hoofdstuk5_Paragraaf_1_Artikel24

Wat zegt de Arbo wetgeving over het verwerken van persoonsgegevens bij een arbeidsongeval?
10. Gelet op artikel 9, tweede lid, onderdeel b, van de Algemene verordening gegevensbescherming, is het verbod om gegevens over gezondheid te verwerken niet van toepassing indien de verwerking geschiedt door de toezichthouder, voor zover de verwerking noodzakelijk is voor het onderzoek naar arbeidsongevallen die leiden tot de dood, een blijvend letsel of een ziekenhuisopname als bedoeld in artikel 9, eerste lid.
11. Indien toepassing wordt gegeven aan het tiende lid worden de gegevens over gezondheid alleen verwerkt door personen die uit hoofde van ambt, beroep of wettelijk voorschrift dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht.

Waarom deze uitzondering op de AVG voor de SZW-inspectie en andere tot geheimhouding gebonden functionarissen?
Van arbeidsongevallen die leiden tot blijvend letsel, een ziekenhuisopname of overlijden moeten werkgevers melding maken bij de Inspectie SZW. Volgend op die melding stelt een inspecteur het onderzoek in naar de oorzaak van het ongeval. Met dat doel spreekt de inspecteur als dat mogelijk is ook met het slachtoffer. In zo'n gesprek zal hij onder meer vragen naar de gezondheid van de werknemer. Op die manier kan hij namelijk achterhalen of de klachten inderdaad zijn ontstaan door het arbeidsongeval. Volgens de Algemene Verordening Gegevensbescherming (AVG) gaat het in zo'n geval om een verwerking van bijzondere persoonsgegevens. En dat is alleen in bepaalde situaties toegestaan. Het verwerken van gegevens over de gezondheid van personen is verboden. Tenzij er een uitzondering uit de AVG van toepassing is. Zo'n uitzondering was er niet voor inspecteurs van de Inspectie SZW. Dit betekende dat zij officieel toestemming zouden moeten vragen aan de werknemer die het slachtoffer is geworden van een arbeidsongeval. Die situatie was niet wenselijk. Want dan zou de werknemer ook de mogelijkheid hebben om geen toestemming te geven. Bijvoorbeeld omdat zijn werkgever druk op hem uitoefent. En dat zou als gevolg hebben dat de Inspectie de werkgever niet kan bestraffen voor een gemaakte fout die tot een ongeval leidt. In het Verzamelwet SZW 2019 is daarvoor een uitzondering opgenomen. Die maakte dat de Inspectie SZW wel gegevens over de gezondheid mag verwerken. Maar uitsluitend personen die door hun beroep zijn gebonden aan geheimhoudingsplicht, mogen deze gezondheidsgegevens verwerken.

Wat heeft dit voor consequenties voor het MAAS incidentenregister?
Arbowet, artikel 9 lid 1. De werkgever meldt arbeidsongevallen die leiden tot de dood, een blijvend letsel of een ziekenhuisopname direct aan de daartoe aangewezen toezichthouder en rapporteert hierover desgevraagd zo spoedig mogelijk aan deze toezichthouder.
Arbowet, artikel 9 lid 2. De werkgever houdt een lijst bij van de gemelde arbeidsongevallen en van arbeidsongevallen welke hebben geleid tot een verzuim van meer dan drie werkdagen en registreert daarop de aard en datum van het ongeval.
Onder 'blijvend letsel' worden ook chronische lichamelijke en psychische klachten verstaan. Onder "ziekenhuisopname" wordt verstaan dat een slachtoffer in een ziekenhuis wordt opgenomen

(Hieronder valt ook een dagopname). Een poliklinische behandeling wordt dus niet als ziekenhuisopname beschouwd.
Ook moet de werkgever het ongeval direct melden zodra bekend is dat er alsnog sprake is van een ziekenhuisopname of van blijvend letsel dat in verband kan worden gebracht met het arbeidsongeval.

Overzicht van verplichtingen voor melden en registreren van ongevallen?
De ettelijke en management systeem verplichtingen m.b.t. het melden en registreren van ongevallen zijn gezien het voorgaande al volgt samen te vatten:

Gevolg ongeval	Melden aan de Arbeidsinspectie (NLA)	Registreren in MAAS ongevallenlijst	Uitzondering AVG op verwerken gezondheidsgegevens
1. Dodelijk ongeval	Ja	Ja	Ja, direct
2. Blijvend letsel	Ja	Ja	Ja, direct
3. Opname in een ziekenhuis	Ja	Ja	Ja, direct
4. Behandeling in ziekenhuis (bijvoorbeeld afdeling Spoedeisende Hulp)	Nee	Ja	Ja, indirect. Kan namelijk later blijken dat toch sprake is van blijven letsel
5. EHBO-behandeling op plaats van ongeval	Nee	Ja	Ja, indirect. Kan namelijk later blijken dat toch sprake is van blijven letsel
6. Ziekteverzuim van minder dan drie werkdagen na een arbeidsongeval	Nee	Ja	Ja, indirect. Kan namelijk later blijken dat toch sprake is van blijven letsel
7. Ziekteverzuim van meer dan drie werkdagen na een arbeidsongeval	Nee	Ja	Ja, indirect. Kan namelijk later blijken dat toch sprake is van blijven letsel

Wat blijft geheel buiten het MAAS incidentenregister?
De Algemene verordening gegevensbescherming (AVG) geeft u de ruimte om de noodzakelijke informatie over uw zieke werknemers vast te leggen. Wat iemand heeft en waardoor dat komt, hoort niet bij deze noodzakelijke informatie.
Gezondheidsgegevens zijn namelijk bijzondere persoonsgegevens. Het verwerken van bijzondere persoonsgegevens is meestal verboden. Daarom mag u er niet naar vragen.
Ook wanneer uw werknemers uit zichzelf vertellen wat zij mankeren, mag u deze informatie niet vastleggen of delen. Of gebruiken om een oordeel te vormen over de inzetbaarheid van uw werknemer. Dat mag alleen de arbodienst of bedrijfsarts. Natuurlijk kunt u uw werknemer wel een luisterend oor bieden.

Type verzuim	Melden aan de Arbeidsinspectie (NLA)	Registreren in MAAS ongevallenlijst	Uitzondering AVG op verwerken gezondheidsgegevens
1. Ziekteverzuim van minder dan drie werkdagen, niet gerelateerd aan een arbeidsongeval	Nee	Nee	Nee
2. Ziekteverzuim van meer dan drie werkdagen, niet gerelateerd aan een arbeidsongeval	Nee	Nee	Nee

112. G&VW. Beroepsziekte melden

Wat zegt de Autoriteit Persoonsgegevens over beroepsziekte?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-en-uitkering/mijn-zieke-werknemer?qa=beroepsziekte&scrollto=1

Wat zeggen andere belanghebbenden over beroepsziekte?
https://www.beroepsziekten.nl/
https://www.beroepsziekten.nl/sites/default/files/documents/stappenplan-melden-beroepsziekte-covid-19-cascode-605.pdf

Wordt corona, opgelopen op het werk, beschouwd als en beroepsziekte ?
COVID-19 kan sinds 1 april 2020 in Nederland worden gemeld als beroepsziekte. Nederland loopt ruim achter op België met het melden van COVID-19 als beroepsziekte. Het vermoeden bestaat dat bedrijfsartsen een besmetting aan het coronavirus tijdens het werk welke aansluitend lijdt tot ziekenhuis opname en mogelijk zelfs tot de dood, dit niet beschouwen als een beroepsziekte.

Moet corona gemeld worden als een beroepsziekte aan het NCvB door de bedrijfsarts?
Ja, indien iemand door het werk, of grotendeels door het werk, ziek is geworden door besmetting aan COVID-19 dan moet dit gemeld worden als beroepsziekte. Het NCVB heeft voor het melden van een beroepsgebonden Corona Virus Ziekte (COVID-19) CAScode R605 aangemaakt. Arbowet Artikel 9.

Welke wettelijke eis aanmelding en registratie van arbeidsongevallen en beroepsziekten?
lid 3: De bedrijfsarts of de arbodienst meldt beroepsziekten aan het NCvB. (vrij vertaald)
Arboregeling Artikel 1.11. Gegevens beroepsziekten
lid 1. In dit artikel wordt verstaan onder beroepsziekte: een ziekte of aandoening als gevolg van een belasting die in overwegende mate in arbeid of arbeidsomstandigheden heeft plaatsgevonden.

Stappenplan?
Er is een stappenplan gemaakt met enkele aanvullende vragen voor het melden van COVID-19 als beroepsziekte en om deze meldingen beter kunnen duiden. Ook is het mogelijk om een groepsmelding voor COVID-19 meldingen te doen. S*tappenplan registratie Corona Virus Ziekte 2019 als beroepsziekte R605*

Is mijn beroepsziekte gemeld?
U kunt als werknemer niet via het Nederlands Centrum voor Beroepsziekten nagaan of uw bedrijfsarts uw beroepsziekte gemeld heeft. Dat komt omdat bedrijfsartsen bij een melding geen gegevens verstrekken die te herleiden zijn tot een individuele patiënt of een specifiek bedrijf. Bedrijfsartsen zijn weliswaar volgens de Arbeidsomstandigheden wet (artikel 9 lid 3) en de Arbeidsomstandighedenregeling (artikel 1.11 lid 1-3) verplicht om een beroepsziekte te melden bij het NCvB, maar dit is alleen voor preventieve doeleinden. De spelregels staan omschreven in stap Vijf van het Zes-stappenplan NCvB (http://www.beroepsziekten.nl/ncvb/stap-5-concluderen-en-melden).
Advies NCvB: Wend u rechtstreeks tot uw bedrijfsarts

113. G&VW. BHV en BHV-gerelateerd incident

Wat zegt de Autoriteit Persoonsgegevens over BHV?
Geen specifieke informatie

BHV benchmark (verwerkingsregister):

- https://www.avgregisterrijksoverheid.nl/Ministerie_van_EZK_en_Ministerie_van_LNV/2492_BHVbedrijfshulpverlening.html
- https://www.avgregisterrijksoverheid.nl/Ministerie_van_Volksgezondheid_Welzijn_en_Sport_/5091_BHV__Voeren_registratie_BHVers.html

Wat betekent de Algemene Verordening Gegevensbescherming (AVG) voor BHV?
Werkgevers mogen met het oog op privacy geen bijzondere persoonsgegevens verwerken. Gegevens over, zeg, de gezondheid van werknemers. Voor algemene persoonsgegevens, zoals naam, adres, et cetera, geldt een minder zware toets. Daarvoor is het in principe voldoende als de gegevens noodzakelijk zijn voor de uitvoering van een wettelijke plicht.

Hoe is de wettelijk plicht rond BHV?

- Artikel 3 van de Arbowet zegt dat de werkgever beleid moet maken dat is gericht op zo goed mogelijke arbeidsomstandigheden. Meer informatie hierover in: artikel 3 lid 1 e.
- Artikel 15 van de Arbowet vermeldt dat de werkgever zich mag laten ondersteunen door deskundige BHV'ers. Hier staat ook beschreven wat de taken van de BHV'ers zijn en de verplichting tot opleiden van de BHV'ers binnen de organisatie.

Mag ik als EHBO'er gegevens van een slachtoffer doorgeven aan de ambulanceverpleegkundigen?
Als je persoonlijke informatie hebt over het slachtoffer mag je dit gewoon delen met de ambulanceverpleegkundigen. De AVG is pas van toepassing als de informatie wordt verwerkt. Dat is of met een computer of op papier als het doel is ze in een database op te nemen. In de praktijk geef je mondeling deze informatie door. Dan speelt de AVG niet. Wat het ambulancepersoneel met de informatie doen is hun zaak. Daar hoef je je als EHBO'er niet druk om te maken.

114. G&VW. Medewerkertevredenheidonderzoek (MTO)

Wat zegt de Autoriteit Persoonsgegevens over MTO?
Geen specifieke informatie

MTO benchmark (verwerkingsregister):
https://www.avgregisterrijksoverheid.nl/Ministerie_van_EZK_en_Ministerie_van_LNV/1348_Meten_medewerkerstevredenheid_SodM_.html

Wat is het doel van de gegevensverwerking voor het Medewerkertevredenheidonderzoek (MTO)?
Het MTO is een onderzoek onder MAAS medewerkers over hoe zij hun werk en werkomgeving beleven en welke effecten dit heeft op hun gezondheid en welbevinden. Het geeft inzicht in de persoonlijke werksituatie, werkplezier, balans tussen werk en privé, leervermogen, mentale en fysieke gezondheid en inzetbaarheid. Er wordt zodoende informatie verzameld voor verbeteringen op thema's binnen het HR-domein. De uitkomsten ervan bieden aanknopingspunten voor acties om de tevredenheid en de betrokkenheid van medewerkers te vergroten. Uiteindelijk draagt dit bij aan een organisatie waar medewerkers duurzaam inzetbaar (kunnen) zijn.

Waarom wordt binnen het Medewerkertevredenheidonderzoek (MTO) gebruik gemaakt van persoonsgegevens?
Dit is noodzakelijk om de gestelde projectdoelen te bereiken. Het uitgangspunt is dat geanonimiseerd wordt daar waar kan. Waar het niet kan wordt gepseudonimiseerd. Is ook dat niet mogelijk dan wordt (zo minimaal mogelijk) gebruik gemaakt van persoonsgegevens ten bate van het onderzoek. Hoe deze afwegingen zijn gemaakt is hieronder uitgewerkt.

Wat is de minimale groepsgrootte om te anonimiseren?
Er wordt alleen gerapporteerd over groepen die groot genoeg zijn, dus waarbij de respons minimaal 10 personen bedraagt.

Waarom zijn PAGO-vragen" (mentale en fysieke gezondheidsvragen) een onderdeel van de vragenlijst?
Hiermee wordt invulling gegeven aan de wettelijke verplichting vanuit de Arbeidsomstandigheden-wetgeving'4. Hierbij stelt "de werkgever (...) de werknemers periodiek in de gelegenheid een onderzoek te ondergaan, dat erop is gericht de risico's die de arbeid voor de gezondheid van de werknemers met zich brengt zoveel mogelijk te voorkomen of te beperken."

Hoe anonimiseren?
Niet alleen de onderzoeksrapportage dient geanonimiseerd opgeleverd te worden, maar ook bij de middelen die je gebruikt om de data te vergaren is het van belang dat een persoon niet identificeerbaar is. Zodra persoonsgegevens niet meer nodig zijn, moeten deze gegevens verwijderd worden. Voor het onderzoek betekent dit dat rapportages geanonimiseerd opgeleverd worden én dat niet meer naar een individu te herleiden is welke antwoorden deze persoon gegeven heeft. Ditzelfde geldt voor de middelen die u gebruikt hebt om uw data te vergaren.

Respondent recht op inzicht in doel?
Een respondent heeft altijd recht op inzicht in het onderzoeksdoel en de onderzoeksorganisatie (en opdrachtgever). Ook moet een plek benoemd worden waar de respondent meer informatie kan vinden. Daarnaast hebben respondenten altijd het recht om informatie die van hen opgeslagen is in

te zien, maar hebben zij ook het recht om ‘vergeten’ te worden en geheel uit systemen verwijderd te worden.

5 belangrijke MTO regels bij Algemene Verordening Gegevensbescherming

1. Bewaar persoonsgegevens niet langer dan noodzakelijk;
2. Verzamel alleen de noodzakelijke persoonsgegevens;
3. Verwerk persoonsgegevens niet voor andere doelen;
4. Geef de respondent inzicht in het onderzoeksdoel, de -organisatie (en opdrachtgever) en de plek waar nadere informatie te vinden is;
5. Zorg ervoor dat een persoon niet identificeerbaar is.

115. G&VW. Ondernemingsraad

Wat zegt de AP over Ondernemingsraad?
https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-uitkering/ondernemingsraad?qa=ondernemingsraad

Benchmark?
https://www.avgregisterrijksoverheid.nl/Ministerie_van_EZK_en_Ministerie_van_LNV/2491_ORgespreks_en_exit_verslagen_.html

Concrete AVG kwesties waarbij instemming van de OR nodig is?
a. interne privacy beleid
b. verwerkingsregister
c. procedure voor het melden van datalekken
d. aanstellen van een Functionaris Gegevensbescherming
e. uitvoeren van een privacy impact assessment

Regeling voor verstrekken van persoonsgegevens?
Als bestuurder van plan is personeelsgegevens te verstrekken, dan moet bestuurder een regeling hiervoor eerst voorleggen aan de ondernemingsraad (OR). De OR heeft wettelijk instemmingsrecht bij voorgenomen verstrekkingen van personeelsgegevens. Dat houdt in dat uw organisatie een regeling hiervoor in principe niet mag vaststellen, veranderen of intrekken zonder instemming van de OR.

Mogen de kandidatenlijsten voor or-verkiezingen mogen binnen de organisatie gepubliceerd worden?
Ja. Om een (wettelijk verplichte) or-verkiezing op zorgvuldige wijze te organiseren is het noodzakelijk kandidatenlijsten te publiceren (als bedoeld in artikel 9 WOR). Hoe kun je anders verkiezingen houden?
Gelet op de AVG is er een gerechtvaardigd belang om te publiceren. Uiteraard moet de or (of verkiezingscommissie) zijn huiswerk doen rond het maken en verspreiden van deze lijsten, zodat deze onvermijdelijke verwerking van persoonsgegevens zorgvuldig geschiedt en de lijsten niet buiten de organisatie terechtkomen. Ook moet de or deze lijsten direct na de verkiezing vernietigen. Of, als dat nodig is, alleen beschikbaar houden voor de verkiezingscommissie.

Mogen we ook lijsten met namen van de kiesgerechtigde en verkiesbare personen verspreiden in de organisatie?
Handel hier terughoudend. Volgens AVG is er een gerechtvaardigd belang om deze lijsten gedurende de verkiezingsperiode te maken en beschikbaar te houden voor de verkiezingscommissie. Zonder de lijsten kan de verkiezingscommissie niet toetsen wie wel of niet geldig hebben gestemd en/of zich geldig kandidaat hebben gesteld. Het is echter niet nodig om deze lijsten te verspreiden onder de medewerkers. Zij hoeven alleen te weten of zij zelf kiesgerechtigde en/of verkiesbaar zijn. De AVG laat niet toe dat deze lijsten worden verspreid in de organisatie zonder voorafgaande goedkeuring van alle medewerkers.

Hoe AVG-proof is de OR?
De OR verwerkt zelf als orgaan persoonsgegevens. Ook de OR heeft een archief in digitale vorm. Denk alleen aan de verslagen van OR en commissievergaderingen en de OV. Maar ook de data die worden verzameld rondom verkiezingen. Daar zitten persoonsgegevens bij die zouden kunnen vallen

onder de noemer privacygevoelig. Denk aan kandidaatstelling van personen, lidmaatschap vakorganisaties, aard en lengte dienstverband, vorm arbeidscontract en eventueel verder meer vertrouwelijke aan personen gerelateerde informatie. Dat verzamelen of registreren van persoonsgegevens kan zich ook voordoen rondom de behandeling van bepaalde inhoudelijke onderwerpen. Al is het maar met een kleine (ogenschijnlijk onschuldige) verwijzing in een verslag.

- Wat of welke informatie (1), over welke personen (2), met welk doel (3) en waar, op welke plek en hoe (4) wordt door de OR bewaard. Bepaal ook wat de bewaartermijn (5) is.
- Grondslag is een wettelijke verplichting, namelijk de Wet op de Ondernemingsraden. Informeren (6) Daarbij geef je aan dat zij het recht hebben een en ander te kunnen inzien of laten corrigeren (7) of zelfs laten verwijderen (8) en hoe desgewenst bezwaar (9) kunnen makenis vastgelegd in MAAS Privacy verklaring.
- OR-bestanden zijn goed afgeschermd (10) en alleen toegankelijk (11) voor die personen die daartoe geautoriseerd zijn.

OR instemming met overgang naar nieuwe arbodienst

Nadat de personeelsdossiers naar de nieuwe werkgever zijn overgegaan, zal in veel gevallen de verkrijger na de overgang van onderneming voornemens zijn de nieuwe werknemers bij zijn eigen arbodienst onder te brengen. Aangezien er voor gezondheidsgegevens nog striktere regels gelden dan voor de ‘niet bijzondere' persoonsgegevens, geldt dat de overgang van de ene arbodienst naar de andere arbodienst niet eenvoudig is. Allereerst zal de ondernemingsraad ex artikel 27 lid 1 onderdeel d WOR moeten instemmen met de overgang naar een andere arbodienst. Vervolgens kunnen alle gegevens waarop geen medisch beroepsgeheim rust, zoals administratieve gegevens, terugkoppelingen aan de werkgever en meldingen aan het UWV, naar de opvolgende arbodienst worden overgedragen. Het overdragen van de gegevens die wél onder het medisch beroepsgeheim vallen, is alleen mogelijk onder strenge voorwaarden. In de eerste plaats dient sprake te zijn van een noodzaak tot het verstrekken van deze gegevens in het kader van de verzuimbegeleiding, bijvoorbeeld omdat het een ‘lopend ziektegeval’ betreft. Tevens moeten de betreffende werknemers van tevoren zijn geïnformeerd over de gegevensverstrekking en moeten zij in gelegenheid zijn gesteld om bezwaar te maken. Het is aan de overdragende arts om te controleren of aan deze verplichting is voldaan, alvorens het dossier over te dragen aan een andere gecertificeerde bedrijfsarts.

116. G&VW. PSA en PSA-gerelateerd incident

Wat zegt de AP over PSA?
Geen specifieke informatie

Verband PSA met AVG
De afkorting PSA staat voor Psychosociale Arbeidsbelasting en is een verzamelterm voor factoren in de arbeidssituatie die stress veroorzaken. In 2018 speelde bij 57% van de gemelde beroepsziekten PSA een rol. Vanuit de Arbowet verplichting om beleid te voeren dat gericht is op het voorkomen of beperken van PSA. De Inspectie SZW controleert steeds strenger op de aanwezigheid van de verplichte Risico- Inventarisatie en -Evaluatie (RI&E) binnen bedrijven waarin PSA als onderdeel dient te zijn opgenomen. Bedrijven die niet aan de RI&E verplichting voldoen, riskeren hoge boetes. Bij de uitvoering van een beleid gericht op het beperken en voorkomen van PSA (psychosociale arbeidsbelasting) kan het voorkomen dat een werkgever persoonsgegevens verwerkt. Bijvoorbeeld als er sprake is van een incident waarbij PSA een rol speelt. Dan mag de werkgever wel algemene persoonsgegevens verwerken, zoals de naam van de betrokken medewerkers. Maar worden er daarnaast ook gezondheidsgegevens verwerkt (bijvoorbeeld de medewerker ervaart spanningsklachten door pesten), dan ligt dat anders. Gezondheidsgegevens zijn immers bijzondere persoonsgegevens. En voor het verwerken van bijzondere persoonsgegevens geldt een verbod. Dat kan alleen worden doorbroken als die verwerking noodzakelijk is voor de uitvoering van een wettelijk voorschrift.

Wat betekent de Algemene Verordening Gegevensbescherming (AVG) voor PSA?
De Autoriteit Persoonsgegevens (AP) heeft zich nog niet concreet uitgelaten over de vraag of werkgevers ook (bijzondere) persoonsgegevens mogen verwerken in het kader van de uitvoering van PSA-beleid. Wel valt er iets af te leiden uit eerdere AP-rapporten over de inzet van alcohol- en drugstesten door werkgevers. En dat is dat de AP van mening is dat er een concrete wettelijke mogelijkheid moet zijn voor werkgevers om bijzondere persoonsgegevens te verwerken voor PSA-beleid. Uniper-zaak: alcohol- en drugstesten alleen vanuit wet. In de zogenaamde Uniper-zaak uit 2016 oordeelde de AP dat werkgevers slechts alcohol- en drugstesten moeten uitvoeren als dat concreet in de wet is vastgelegd. Denk bijvoorbeeld aan piloten, machinisten en schippers. En ook alleen dan bijzondere persoonsgegevens mogen verwerken over de gezondheid van werknemers. Maar voor beroepen en functies waarvoor zo'n mogelijkheid niet in de wet is opgenomen (veruit de grootste groep) geldt deze uitzondering niet. In die gevallen mogen werkgevers dus geen alcoholtests laten uitvoeren.

Is er jurisprudentie?
Op 21 maart 2019 heeft de Rechtbank Amsterdam uitspraak gedaan in een zaak die was aangespannen door een werkneemster tegen haar voormalige werkgever en een door de werkgever ingeschakeld onderzoeksbureau. De werkgever had na gefundeerde klachten over de werkneemster, onderzoek laten verrichten naar haar gedrag. De werkneemster vorderde o.a. een schadevergoeding en vernietiging van alle over haar verzamelde persoonsgegevens. De rechtbank oordeelde dat de werkgever een gerechtvaardigd belang had voor het verrichten van het onderzoek, te weten het voorkomen dan wel beperken van psychosociale arbeidsbelasting. Werkgevers zijn, onder meer op grond van artikel 3 Arbowet en artikel 7:611 BW, gehouden om maatregelen te treffen tegen ongewenst gedrag op de werkvloer. De inbreuk die met het onderzoek op de persoonlijke levenssfeer van de werkneemster werd gemaakt, is gerechtvaardigd door de wettelijke plicht van de werkgever om zorg te dragen voor een veilige en gezonde werkomgeving voor haar werknemers.
Bronnen:

- https://www.loyensloeff.com/nl/nl/nieuws/nieuwsartikelen/onderzoek-naar-wangedrag-werkneemster-niet-in-strijd-met-de-avg-n14554/
- https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2019:2166
- https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBNHO:2019:4283
- https://www.ploum.nl/rechterlijke-avg-uitspraken/

Welk wettelijk kader bij afweging tussen verrichten van onderzoek en privacybelangen werknemer?

Uit de beoordeling van de Rechtbank Amsterdam volgt welke stappen een werkgever moet nemen voorafgaand aan het instellen van een onderzoek:

1. Heeft de werkgever een grondslag voor het verwerken van de persoonsgegevens?
   Het verwerken van persoonsgegevens is alleen rechtmatig wanneer de verwerker hier een grondslag voor heeft, zoals limitatief opgenomen in artikel 6 lid 1 sub a tot en met f AVG. Bij een onderzoek naar de gedragingen van een werknemer zal veelal (net zoals in deze zaak) de verwerkingsgrondslag zijn gelegen in een noodzakelijke verwerking voor de behartiging van de gerechtvaardigde belangen van de werkgever en (een) derde(n) (in deze zaak de betrokken werknemer). Het gerechtvaardigd belang was in deze zaak gelegen in de plicht van de werkgever op grond van artikel 3 Arbowet om zorg te dragen voor de veiligheid en gezondheid van haar werknemers. De rechtbank Amsterdam oordeelde dat aangezien de werkgever een melding van ongewenst gedrag had ontvangen van een werknemer, zij als werkgever een gerechtvaardigd belang had om opdracht te verstrekken voor het doen van het onderzoek naar het gedrag van werkneemster. De Rechtbank Amsterdam achtte het niet van belang dat werkneemster haar toestemming tot het verwerken van haar persoonsgegevens had ingetrokken, aangezien niet de toestemming van de werkneemster maar het gerechtvaardigd belang van de werkgever de verwerkingsgrondslag vormde.
2. Weegt dit belang zwaarder dan de grondrechten, belangen of fundamentele vrijheden van de betrokkene?
   Het gerechtvaardigd belang van de werkgever (en haar werknemer) kan alleen als geldige verwerkingsgrondslag dienen, indien dit belang zwaarder weegt dan de grondrechten, belangen of fundamentele vrijheden van de werkneemster, rekening houdend met de redelijke verwachtingen van de betrokkene op basis van zijn verhouding met de verwerkingsverantwoordelijke. De rechtbank zet de belangen van de werkneemster en werkgever naast elkaar: het recht van de werkneemster op respect voor haar privéleven (artikel 8 EVRM), versus de plicht van de werkgever om op grond van artikel 3 Arbowet zorg te dragen voor de veiligheid en gezondheid van haar werknemers en de plicht om zich als goed werkgever te gedragen (artikel 7:611 BW). De rechtbank stelt dat in deze afweging een inbreuk op het recht op respect voor het privéleven is toegestaan, mits wordt voldaan aan de eisen van proportionaliteit en subsidiariteit.
3. Wordt voldaan aan de eisen van proportionaliteit en subsidiariteit?
   De rechtbank betrekt bij het beoordelen van de proportionaliteit dat werkgever wettelijk verplicht was om de gegrondheid van de klachten over werkneemster nader te onderzoeken. De rechtbank neemt hierbij in zijn overweging mee dat het grensoverschrijdend gedrag van de werkneemster door het sturen van WhatsApp-berichten en e-mails naar het privé e-mailadres van de werknemer ook buiten werktijd en in de privésfeer plaatsvond. Het vermoeden dat sprake was van grensoverschrijdend gedrag was concreet weergegeven in de formele klachten en de grensoverschrijdende gedragingen zouden herhaaldelijk, over enkele maanden hebben plaatsgevonden. Onder deze omstandigheden heeft werkgever redelijkerwijs tot het doen van het onderzoek en het verwerken van de persoonsgegevens kunnen komen.

   Bij het beoordelen van de subsidiariteit acht de rechtbank het van belang dat er voorafgaand aan het instellen van het onderzoek gesprekken hebben plaatsgevonden met de werkneemster. Ook oordeelt de rechtbank dat de werkgever op een passende wijze is

omgegaan met de persoonsgegevens van werkneemster, door niet zelf onderzoek te doen maar een onafhankelijk onderzoeksbureau in te schakelen. Het was in het belang van werkneemster dat de klachten op onafhankelijke wijze zouden worden onderzocht. Het is niet gebleken dat er andere, minder ingrijpende middelen voorhanden waren om het onderzoeksdoel te realiseren en de rechtbank komt hiermee tot de conclusie dat ook aan het subsidiariteitsvereiste is voldaan.

Alle vorderingen van werkneemster worden afgewezen.

4. Conclusie.

Uit deze zaak blijkt dat wanneer werkgevers worden geconfronteerd met gegronde klachten over het gedrag van werknemers, zij een wettelijke plicht hebben op grond van artikel 3 Arbowet en artikel 7:611 BW om iets met deze klachten te doen. Deze wettelijke plicht biedt werkgevers ook direct een verwerkingsgrondslag onder AVG voor het (laten) uitvoeren van een onderzoek. Belangrijk hierbij is om goed oog te hebben voor de proportionaliteit en subsidiariteit; de klachten moeten gefundeerd zijn en er moet zorgvuldig worden gehandeld. Ook zouden er geen minder ingrijpende middelen voorhanden moeten zijn.

117. G&VW. Temperatuur meten

Wat zegt de AP over temperatuur meten?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona/temperaturen-tijdens-corona?qa=temperatuurmetingen&scrollto=1

Wat zeggen anderen?
https://www.ploum.nl/temperatuur-opmeten-van-bezoekers-en-werknemers-mag-dat/

Mag je de lichaamstemperatuur opmeten van iedereen die toegang wil tot het pand of het bedrijfsterrein?
Voor de coronacrisis nemen veel bedrijven maatregelen om zo veilig mogelijk te werken en de verspreiding van het coronavirus tegen te gaan. Voor sommige beroepen is thuiswerken goed mogelijk, maar er zijn ook sectoren waarin het nodig blijft of wenselijk is dat werknemers, leveranciers, klanten, opdrachtnemers en andere bezoekers toch (of: weer) op de werkplek (zullen) verschijnen.

Is het meten van iemands lichaamstemperatuur een verwerking van persoonsgegevens is, waardoor de Algemene Verordening Gegevensbescherming (AVG) van toepassing is?
Verwerking kan slaan op veel verschillende handelingen met een persoonsgegeven: denk aan het inzien, opslaan, doorgeven, bekijken of verwijderen van persoonsgegevens. Het enkele bekijken van een temperatuur op een thermometer of middels een thermische camera, zonder dat de temperatuur wordt opgeslagen of genoteerd of de meetgegevens in een geautomatiseerd systeem terecht komen (bijvoorbeeld dat de werknemer wordt ziek gemeld of dat een automatisch toegangspoortje bij een te hoge temperatuur niet open gaat), is volgens de Autoriteit Persoonsgegevens geen verwerking van persoonsgegevens in de zin van de AVG. Dat wil trouwens niet zeggen dat er dus geen privacy-bezwaren kleven aan het meten van de temperatuur: dat kan bijvoorbeeld nog steeds strijd opleveren met het meer omvattende grondrecht op de persoonlijke levenssfeer. Er moet dus nog altijd een goede belangenafweging worden gemaakt, met inachtneming van allerlei relevante omstandigheden.
Of er sprake is van een verwerking van persoonsgegevens, is contextafhankelijk. Zodra er iets wordt genoteerd of anderszins geregistreerd m.b.t. de temperatuur van een persoon, of dus bijvoorbeeld een poortje niet open gaat, zal sprake zijn van een verwerking van persoonsgegevens en is de AVG van toepassing. Er is waarschijnlijk geen sprake van een verwerking als de temperatuur van personen wordt gescand met thermische camera's in publieke ruimtes, zonder dat er verder (direct of indirect) gegevens worden geregistreerd van de betrokkenen; bijvoorbeeld in een warenhuis. In een ziekenhuis of vliegveld is de kans op verwerken bij zo'n meting al groter, en op een kantoor met 25 werknemers zou van een verwerking nog eerder sprake kunnen zijn, omdat er vaak een registratie aan wordt gekoppeld en de gegevens makkelijker te herleiden zijn naar de betrokken persoon.

Is het meten van iemands lichaamstemperatuur een bijzondere persoonsgegeven?
Als er sprake is van een verwerking en (dus) de AVG van toepassing is, is van belang dat het gaat om gegevens over iemands gezondheid. Er is dan sprake van bijzondere persoonsgegevens en daarvoor geldt in beginsel een verwerkingsverbod. Het uitgangspunt is dat het meten van temperaturen alleen is toegestaan als de uitkomst niet wordt verwerkt. Dat is – na een eerder, nog strenger standpunt van de AP – inmiddels de opvatting (in Nederland). Wil een bedrijf de lichaamstemperatuur wel vastleggen, dan mag dat alleen als men zich kan beroepen op een wettelijke uitzondering voor het verwerken van bijzondere persoonsgegevens.

Uitzondering voor het opmeten van lichaamstemperatuur?
De vraag is dus of er een wettelijke uitzondering is, die het ondernemers mogelijk maakt om de temperatuur van hun werknemers en bezoekers op te meten als de AVG van toepassing is.
Een werkgever mag alleen persoonsgegevens over de gezondheid van zijn medewerkers verwerken als dat noodzakelijk is voor de loondoorbetaling en re-integratie. Een werkgever mag dus wel weten dat werknemer Jansen ziek is en niet kan tillen, maar niet wat Jansen precies mankeert (bijvoorbeeld een hernia). Een werkgever mag ook niet op de stoel van de bedrijfsarts gaan zitten en zelf een diagnose stellen op basis van eigen onderzoek, zoals een alcohol- en drugstest of een temperatuurmeting. Zelfs als de werknemer uit zichzelf vertelt wat hem of haar mankeert, mag een werkgever dat niet registreren.
Een andere uitzondering op voornoemd verwerkingsverbod die wordt genoemd in de AVG, is een verwerking van gezondheidsgegevens die noodzakelijk is “om redenen van algemeen belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid”. Deze uitzondering stelt echter als eis dat er nationale wetgeving moet zijn die deze specifieke verwerking regelt, met inachtneming van het medisch beroepsgeheim en het recht op privacy van de betrokkene. Dergelijke wetgeving is er in Nederland (nog) niet. Van deze uitzondering kunnen werkgevers dus ook geen gebruik maken.
De wettelijke uitzondering die wij ook zo nu en dan voorbij zien komen in dit kader, namelijk een verwerking ten behoeve van “de bescherming van vitale belangen van de betrokkene”, is in dit geval ook niet van toepassing. Het moet dan namelijk gaan om een situatie waarin een betrokkene geen toestemming kan geven, bijvoorbeeld omdat hij bewusteloos is. Bovendien kan men zich afvragen of het hier gaat om belangen van de betrokkene zelf (nee, vinden wij).
Tot slot nog een bekende uitzondering: de uitdrukkelijke toestemming van de betrokkene. Deze toestemming voor de verwerking moet vrij, specifiek, geïnformeerd en ondubbelzinnig zijn. In de relatie werkgever-werknemer wordt aangenomen dat een werknemer vrijwel nooit vrije toestemming kan geven – hij is immers afhankelijk van zijn werkgever. Er is dan geen sprake van rechtsgeldige toestemming, zodat ook deze uitzondering niet van toepassing is. Dit verschilt overigens wel per land.

Temperatuur meten op de werkplek?
Binnen een onderneming zal het vaak nodig zijn om aanvullende gegevens te registreren en/of consequenties te verbinden aan de uitslag van de meting. Denk aan een werknemer die bij de poort wordt geweigerd wegens een te hoge temperatuur. Niet alleen wordt hem de toegang tot de werkplek ontzegd, ook zullen waarschijnlijk aanvullende gegevens worden vastgelegd. Wellicht registreert de werkgever hem als afwezig of ziek, of belandt de werknemer op een lijst met werknemers die tijdelijk geen toegang krijgen tot het werk. In dit scenario gaat het dan niet meer om het enkel aflezen van de temperatuur van een (anoniem) persoon, maar worden er verdere gegevens vastgelegd over een bepaald individu, juist doordat diens temperatuur is gemeten door de werkgever. Dat is in principe niet toegestaan.
Volledigheidshalve vermelden wij hierbij nog dat ook als in een specifiek geval geen sprake is van een ‘verwerking’ van persoonsgegevens in de zin van de AVG, zeker in het kader van een werkgever-werknemersrelatie andere wetgeving bestaat waar rekening mee moet worden gehouden bij de toepassing van dit soort maatregelen.

Temperatuur meten voor leveranciers, klanten en andere bezoekers?
Voor andere betrokkenen die aanwezig zijn op de werkplek, geldt grotendeels hetzelfde. Er is (nog) geen nationale wetgeving die het mogelijk maakt om bezoekers en klanten te testen op lichaamstemperatuur. Ook hier geldt echter dat de beoordeling afhankelijk is van de specifieke omstandigheden van het geval.
Uitdrukkelijke toestemming van deze categorieën van betrokkenen zou in zeer specifieke gevallen een optie kunnen zijn, maar alleen als die toestemming echt volledig vrij is. Dat betekent onder andere dat de betrokkene geen negatieve consequenties mag ondervinden van het feit dat hij geen toestemming geeft. In de praktijk zal dit vaak lastig zijn. Denk aan een vrachtwagenchauffeur die aan de poort wordt gevraagd of hij zich wil laten testen. Hij zal zich waarschijnlijk in meerdere of mindere mate gedwongen voelen om in te stemmen, omdat hij anders het terrein niet op mag en daardoor zijn werk niet kan doen. Dat zou bovendien tot arbeidsrechtelijke consequenties kunnen leiden bij zijn eigen werkgever. Zijn toestemming is dan niet rechtsgeldig – want niet vrijelijk – gegeven. Het is lastig om een scenario te bedenken waarin toestemming wél vrijelijk wordt gegeven, omdat de meeste bedrijven toch graag selectie aan de poort uitvoeren, voordat zij bezoekers toelaten in het pand of op hun terrein.

Koppeling met andere gegevens?
Binnen een organisatie met werknemers en bezoekers zal er vaak een koppeling plaatsvinden met andere persoonsgegevens, en wordt er niet uitsluitend en eenmalig een temperatuur afgelezen. Daarmee is de AVG van toepassing en zal – gezien het ontbreken van een passende wettelijke uitzondering op het verwerkingsverbod van medische gegevens – het meten van temperatuur als toegangscontrole veelal niet zijn toegestaan.
Als er al een beroep zou kunnen worden gedaan op een wettelijke uitzondering, in een specifiek geval, geldt ook nog dat het verwerken van gezondheidsgegevens in beginsel alleen voorbehouden is aan artsen. Bovendien moet de betreffende verwerking dan ook noodzakelijk zijn voor het beoogde doel. Dat is afhankelijk van de concrete omstandigheden, maar daar zijn in veel gevallen ook vraagtekens bij te plaatsen. Zo is het bijv. de vraag of men niet kan volstaan met vertrouwen in eigen werknemers: verzoeken om de eigen temperatuur dagelijks te meten; dat mag wél. En is het meten van temperaturen wel een passend middel om het doel, de verspreiding van het coronavirus, tegen te gaan? Inmiddels is immers gebleken dat ook personen zonder klachten het virus kunnen verspreiden, terwijl de werknemers anderszins juist een vals gevoel van veiligheid zouden kunnen krijgen doordat zij en hun collega's door de test zijn gekomen.
Uitsluitend wanneer een temperatuurmeting niet gepaard gaat met een registratie en/of in een geautomatiseerd systeem terecht komt, is deze meting (behoudens andere regelgeving, waarop dus ook altijd gecontroleerd moet worden) toegestaan.

Wat is er wel mogelijk als de AVG van toepassing is?
Allereerst is het natuurlijk belangrijk te toetsen of sprake is van een 'verwerking van persoonsgegevens' in de zin van de AVG. Is dat het geval (en naar onze mening is dat al snel zo), dan is het meten van temperatuur door ondernemers veelal niet toegestaan. Natuurlijk kunnen ondernemers dan wel andere acties ondernemen om hun personeel en bezoekers zo veilig mogelijk te houden. We adviseren dat ook ten zeerste te doen: een werkgever moet zorgen voor een veilige werkomgeving. Zo is het van groot belang om de instructies van het RIVM op te blijven volgen en werknemers en bezoekers hier continu over te informeren.

118. G&VW. Vakbond

Wat zegt de AP over Vakbond?
https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens?qa=vakbond&scrollto=1

Een van de vakbonden die is aangeschreven in verband met aankomende OR-verkiezingen stelt recht te hebben op de medewerkerslijsten van MAAS. Is dat zo en is dat geen schending van de privacyregels?
Een kandidatenlijst voor de verkiezing van de OR kan onder meer worden ingediend door een vakbond die aan de genoemde eisen voldoet in artikel 9 van de Wet op de Ondernemingsraden. Als er verkiezingen aankomen, sturen de meeste OR's een brief aan de vakbonden met daarin de naam en adres van het bedrijf, de verkiezingsdatum en de datum waarop de bereidverklaringen van de kandidaten die de vakbonden willen stellen, bij de or binnen moeten zijn. Vakbonden verzoeken OR's regelmatig om ook de lijst met verkiesbare medewerkers mee te sturen, die hen in staat stelt alleen de in de betreffende onderneming werkzame verkiesbare vakbondsleden uit te nodigen om zich kandidaat te stellen. Aangezien de vakbonden contact moeten kunnen opnemen met deze werknemers, is de verwachting dat in ieder geval naam en contactgegevens worden verstrekt. Wel moet de OR de medewerkers tijdig informeren over de verstrekking van deze persoonsgegevens aan de vakbond en hen daarbij in de gelegenheid stellen om daartegen bezwaar te maken binnen een redelijke termijn (bijvoorbeeld een of twee weken). Overigens mogen de vakbonden deze personeelsgegevens alleen gebruiken voor het aanschrijven van hun leden in het kader van de OR-verkiezingen. Na het aanschrijven van hun leden dienen de vakbonden de lijst met personeelsgegevens weer te vernietigen. Onder de AVG geldt een documentatieplicht. Op grond daarvan moeten organisaties kunnen aantonen dat zij bij de verwerking van persoonsgegevens voldoen aan de beginselen van rechtmatigheid, transparantie, doelbinding en juistheid.

Vergoeding vakbondscontributie aan werknemer?
Werkgever mag het lidmaatschap van de vakbond alleen verwerken voor het doel waarvoor de werknemer toestemming heeft gegeven. Zo kan werkgever bijvoorbeeld naar het lidmaatschap kunnen vragen als hij een vergoeding voor (een deel van) de vakbondscontributie aan de werknemer wil betalen. Hij kan dan vragen of leden van een vakbond zich willen melden als zij van deze vergoeding willen profiteren. Het is voor de werkgever dan verstandig daarbij te vermelden dat het vakbondsleden vrijstaat om zich wel of niet te melden, dat zij op elk gewenst moment hun toestemming weer kunnen intrekken en dat het gegeven alleen voor de vergoeding gebruikt wordt.

119. G&VW. Vertrouwenspersoon

Wat zegt de AP over Vertrouwenspersoon?
https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/personeelsgegevens/doorgeven-van-personeelsgegevens

Wat vereist de AP bij doorgeven informatie over ongewenst gedrag
Is er een klacht tegen een van uw werknemers ingediend over ongewenst gedrag, zoals seksueel grensoverschrijdend gedrag? Dan verzamelt een klachtencommissie of vertrouwenspersoon gevoelige informatie over uw werknemer. Hiermee moet deze commissie of persoon zorgvuldig omgaan.
Tijdens de klachtenprocedure is nog niets bewezen. Dat betekent dat de klachtencommissie of vertrouwenspersoon zeer terughoudend moet zijn met het doorgeven van informatie.
Of de direct-leidinggevende van de betreffende werknemer informatie moet krijgen over een lopende klachtenprocedure, verschilt per geval. Dit hangt onder meer af van de aard en de ernst van het ongewenste gedrag. En of het gedrag (ook) plaatsvindt op de afdeling van de leidinggevende.
Als de klacht gegrond is verklaard, brengt de klachtencommissie of vertrouwenspersoon de leidinggevende van de uitspraak op de hoogte.

Welke bewaartermijn bij klacht over ongewenst gedrag?
Een redelijke bewaartermijn voor de informatie van de klachtencommissie of vertrouwenspersoon is maximaal 2 jaar nadat de klacht is afgehandeld. Het is niet nodig deze informatie oneindig te bewaren. Het is belangrijk dat u als werkgever hiervoor een duidelijke bewaartermijn afspreekt.

Wat opgeslagen in personeelsdossier?
Het oordeel van de klachtencommissie of vertrouwenspersoon kunt u in het personeelsdossier van de betreffende werknemer bewaren.

Wat betekent de Algemene Verordening Gegevensbescherming (AVG) voor de verslaglegging van in- en externe vertrouwenspersonen? Bron: Hubert Consult/dr. mr. Marlies Vegter

- https://www.hubertconsult.nl/avg-implicaties-vertrouwenspersonen/
- https://hetvolstevertrouwen.nl/read/5-vragen-over-de-vertrouwenspersoon?sublist=24188
- https://www.lvvv.nl/

Kort samengevat: Vertrouwenspersonen moeten hun administratie op orde hebben en desgevraagd inzage kunnen geven in de manier waarop zij persoonsgegevens verwerken en de maatregelen die zij nemen om misbruik te voorkomen. Persoonlijke aantekeningen vallen onder de AVG, als deze op een gestructureerde manier worden verwerkt. Het is echter niet vereist om een aangeklaagde te informeren over of inzage te geven in dergelijke aantekeningen, als dit in strijd zou zijn met de geheimhoudingsplicht/ het beroepsgeheim van de vertrouwenspersoon. De bescherming van de klager weegt dan zwaarder.

Is de AVG ook relevant voor vertrouwenspersonen?
Ja, verantwoordingsplicht. Is een vertrouwenspersonen in dienst van een organisatie, dan heeft in principe de organisatie de verantwoordingsplicht en niet de vertrouwenspersoon zelf. Dit kan anders zijn als vertrouwenspersonen, ook al zijn zij in dienst bij een werkgever, zelf bepalen welke persoonsgegevens zij bewaren, voor welk doel en op welke manier. Is dat het geval, dan zijn deze vertrouwenspersonen ook verwerkingsverantwoordelijke en moeten zij aan de eisen van de AVG voldoen. Belangrijk in dit verband is dat de verwerkingsverantwoordelijke inventariseert welke

gegevens hij/zij of de organisatie verwerkt en een verklaring opstelt hoe met deze gegevens wordt omgegaan.

Moeten aantekeningen die vertrouwenspersonen maken over cliënten die hen als vertrouwenspersoon benaderen op een specifieke manier bewaard worden en welke rechten hebben cliënten met betrekking tot inzage, verwijdering, enz.
In beginsel hebben alle mensen van wie persoonsgegevens worden verwerkt, een inzagerecht, een recht op correctie van de gegevens, het recht om de gegevens te laten verwijderen en het recht om de gegevens 'mee te nemen'. Persoonsgegevens zijn alle gegevens die betrekking hebben op een persoon. De AVG is echter alleen van toepassing, als sprake is van verwerking van persoonsgegevens. Dat is het geval wanneer persoonsgegevens zijn opgenomen in een bestand of het de bedoeling is dat dat zal gebeuren en/of wanneer de gegevens geautomatiseerd worden verwerkt. Zuiver persoonlijke aantekeningen vallen niet onder het inzagerecht evenmin als wat losse papieren op het bureau met daarin wat namen of een puur mondelinge overdracht van gegevens. Zodra er structuur wordt aangebracht in de gegevens is de AVG echter van toepassing.
Voor vertrouwenspersonen betekent dit dat aantekeningen van gesprekken met cliënten niet onder de AVG vallen als het puur persoonlijke aantekeningen zijn waar verder niets mee gebeurt. Zodra de aantekeningen echter worden bijgehouden, bijvoorbeeld ten behoeve van een geanonimiseerd jaarverslag of simpelweg om overzicht te houden, is de AVG van toepassing. Het maakt daarbij niet uit of de aantekeningen alleen op papier worden bewaard of ook in de computer.
Is de AVG van toepassing, dan hebben de personen van wie gegevens worden opgeslagen, de hiervoor genoemde rechten op inzage, correctie, wissen en meenemen van gegevens. Deze rechten komen in elk geval toe aan degenen die met de vertrouwenspersoon hebben gesproken over ongewenst gedrag op het werk en over het mogelijk indienen van een klacht.

Hebben aangeklaagden die rechten ook?
In beginsel heeft ook de potentiële aangeklaagde de rechten. Ook daarvan worden immers persoonsgegevens verwerkt. Dat zou betekenen dat een aangeklaagde inzage kan verlangen in de aantekeningen die een vertrouwenspersoon naar aanleiding van een klacht heeft gemaakt.
De aangeklaagde moet dan wel weten dat die gegevens verwerkt worden. Hoofdregel van de AVG is dat betrokkenen er over geïnformeerd moeten worden dat hun gegevens worden verwerkt. Worden diens gegevens echter buiten iemand om verkregen, dan hoeft die persoon daar niet over ingelicht te worden als de persoonsgegevens vertrouwelijk moeten blijven in verband met een beroepsgeheim/ geheimhoudingsplicht. Op deze grond kan een vertrouwenspersoon er dus vanaf zien om een potentiële aangeklaagde te laten weten dat zijn/haar persoonsgegevens worden verzameld.
Weet de aangeklaagde al dat zijn gegevens voorkomen in een verslag van de vertrouwenspersoon en vraagt hij daarin inzage, dan kan dit geweigerd worden op de grond dat dit noodzakelijk is ter waarborging van de bescherming van de rechten en vrijheden van de klager. Het recht op inzage en de andere rechten die de AVG biedt, gelden in een dergelijk geval namelijk niet of in beperktere mate. De vertrouwenspersoon moet desgevraagd wel kunnen uitleggen waarom hij inzage heeft geweigerd en hoe hij de belangen van klager en aangeklaagde tegen elkaar heeft afgewogen.

Mag de vertrouwenspersoon privacygevoelige informatie delen, en zo ja: met wie en wanneer?
Per klacht maakt de vertrouwenspersoon een dossier aan met daarin:

- Persoonsgegevens van de klager.
- Persoonsgegevens van de aangeklaagde.
- Beschrijving van de inhoud van de klacht.
- Verslagen van gesprekken.

Het dossier van de vertrouwenspersoon valt onder de AVG. De vertrouwenspersoon mag alleen feiten en omstandigheden die betrekking hebben op de klacht registreren. Het registreren van bijzondere persoonsgegevens – zoals seksuele voorkeur, levensovertuiging, godsdienst, ras of gezondheid – is alleen toegestaan als dit rechtstreeks betrekking heeft op de klacht.
De klager moet uitdrukkelijk toestemming geven voor het aanmaken van een dossier. Puur persoonlijke aantekeningen van de vertrouwenspersoon vallen niet onder de AVG als er verder niets mee gebeurt. Zodra de vertrouwenspersoon aantekeningen verwerkt of deelt, bijvoorbeeld in een jaarverslag of een dossier, vallen deze gegevens onder de AVG.

Waarom is registratie door vertrouwenspersoon in bepaalde gevallen noodzakelijk en welke doelen heeft de registratie?
Het registreren van (persoons)gegevens door de vertrouwenspersoon is noodzakelijk voor een correcte en adequate afhandeling van een klacht. Daarnaast heeft registratie tot doel:

- In kaart brengen van de klacht.
- Volgen van het afhandelingsproces van de klacht.
- Feitenverzameling in geval een klacht ingediend wordt bij bevoegd gezag of de klachtencommissie.
- Feitenverzameling in geval meerdere klachten over een aangeklaagde binnenkomen.
- (Veel) voorkomende ongewenste omgangsvormen in kaart brengen/incidentenregistratie.
- Gegevensverzameling ten behoeve van het jaarverslag van de vertrouwenspersoon voor het bevoegd gezag.
- Tijdsregistratie ten behoeve van de verantwoording van het werk van de vertrouwenspersoon aan het bevoegd gezag.

Wat is zorgvuldig?
Van de vertrouwenspersonen mag verwacht worden, dat hij of zij uiterst zorgvuldig omgaat met de geregistreerde informatie:

- De vertrouwenspersoon bewaart dossiers en (digitale) gegevensdragers met klachtgegevens achter slot en grendel.
- De computer is beveiligd met een wachtwoord dat alleen bij de vertrouwenspersoon bekend is.
- Indien de vertrouwenspersoon dossiers in een cloud-omgeving opslaat, mag niemand anders dan de vertrouwenspersoon zelf daar toegang toe hebben.
- De vertrouwenspersoon bespreekt dossiers niet met anderen; ook niet met collega-vertrouwenspersonen. Bij intervisie kunnen vertrouwenspersonen een dossier geanonimiseerd bespreken; hierbij mogen de persoonsgegevens niet herleidbaar zijn.
- De vertrouwenspersoon bewaart gegevens niet langer dan voor het doel noodzakelijk is. Er is op grond van de AVG geen concrete bewaartermijn voor dossiers van vertrouwenspersonen. Gebruikelijk is om dossiers na het afsluiten van een klachttraject en verwerking in het (geanonimiseerde) jaarverslag te vernietigen.
- De vertrouwenspersoon draagt lopende dossiers over aan zijn/haar opvolger. Ook hierbij gaat het enkel om noodzakelijke informatie.

Wat houdt inzage en correctierecht voor vertrouwenspersoon?
Klager heeft het recht op inzage van de gegevens (klachtdossier). Daarnaast heeft klager het recht om wijzigingen te laten aanbrengen en/of gegevens te laten verwijderen. Dit inzagerecht omvat inzage in het complete dossier, behalve persoonlijke aantekeningen. Dit geldt overigens voor iedereen van wie persoonsgegevens in het klachtdossier zijn opgenomen, dus ook een aangeklaagde. De vertrouwenspersoon moet altijd inzage geven, tenzij de veiligheid van de klager in

gevaar komt. Wanneer de vertrouwenspersoon inzage weigert, moet iemand met beslissingsbevoegdheid dit goed hebben afgewogen en goed kunnen onderbouwen. Ook moet vertrouwenspersoon deze weigering schriftelijk vastleggen.

Verder kan de vertrouwenspersoon in drie gevallen noodzakelijke gegevens verstrekken en inzage geven in het dossier. Die drie gevallen zijn:

1. Diegene die belast is met klachtbehandeling, leiding geeft en/of anderszins betrokken is bij de behandeling van de klacht. De vertrouwenspersoon moet beoordelen of inzage in het klachtdossier noodzakelijk is en welke gegevens hij verstrekt.
2. Degene die toestemming heeft gekregen van de klager/aangeklaagde om de gegevens in te zien/te ontvangen. De vertrouwenspersoon moet beoordelen of toestemming niet onder druk is gedaan.
3. Justitie en/of politie in het geval van aangifte en/of strafbare feiten.

120. G&VW. Klokkenluider

Wat zegt de AP over Klokkenluider?

- https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_implementatie_klokkenluidersrichtlijn.pdf

Andere bronnen

- https://www.wetbeschermingklokkenluiders.nl/
- https://www.wetbeschermingklokkenluiders.nl/wat-verandert-er/externe-meldkanalen
- https://www.wetbeschermingklokkenluiders.nl/wat-verandert-er/betere-bescherming-klokkenluiders
- https://www.wetbeschermingklokkenluiders.nl/wat-verandert-er/strengere-eisen-interne-meldprocedure

AVG bij doorzendplicht?
De autoriteiten hebben nu al een doorzendplicht. Het doorzenden van de melding moet ook al voldoen aan de eisen van de AVG (bescherming persoonsgegevens). In de Wet bescherming klokkenluiders is de geheimhoudingsplicht van de identiteit van de melder aangescherpt. et personeel dat de meldingen behandelt moet daartoe worden opgeleid, en alleen deze personen hebben toegang tot de informatie. Zij dienen de identiteit van de melder geheim te houden, tenzij de melder toestemming geeft om zijn identiteit bekend te maken.

AVG en omgaan met gegevens van de melding?
De werkprocessen moeten zo ingericht zijn, dat aan de geheimhoudingsplicht en feedbackplicht kan worden voldaan. Als een melding niet bij het juiste (bevoegde) personeelslid (van het externe meldpunt) terechtkomt, moeten de gegevens veilig en volgens de regels van de AVG worden overgedragen aan de bevoegde personen. Daarnaast moeten autoriteiten die (ook) meldingen over het Unierecht behandelen binnen zeven dagen een ontvangstbevestiging op de melding geven én binnen drie tot zes maanden informatie bieden over de stand van zaken en eventuele vervolgacties.

AVG en samenwerking met andere toezichthouders
Soms hebben meldingen betrekking op meerdere rechtsgebieden. Dat betekent dat er verschillende autoriteiten bij betrokken kunnen zijn. Samenwerking is daarom heel belangrijk. Denk aan een melding die deels over het milieurecht gaat, en deels over de AVG. In de werkwijze van autoriteiten zou een samenwerkingsprotocol goed passen als meldingen vaker raakvlakken hebben met dezelfde organisaties. In incidentele gevallen kunnen ook afspraken gemaakt worden over een specifieke melding die meerdere organisaties raakt. Daarbij is het ook belangrijk dat uitwisseling van (persoons)gegevens tussen die autoriteiten op een correcte manier gebeurt. Hiervoor is een juridische grondslag vastgelegd in het wetsvoorstel.

121. Beleidsregels. Aansprakelijkheid & AVG

Wat zegt de AP over Aansprakelijkheid?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/functionaris-gegevensbescherming-fg?qa=aansprakelijkheid&scrollto=1

Wat is de aansprakelijkheid B2B onder de AVG?
Aansprakelijkheid voor financiële schade die een opdrachtgever lijdt als een door hem ingeschakelde verwerker de AVG schendt of de afspraken uit het gesloten verwerkerscontract niet, niet tijdig of niet volledig nakomt. Het is juridisch volkomen toegestaan dat de eventuele aansprakelijkheid van de leverancier op dit vlak tegenover zijn opdrachtgever wel beperkt wordt, bijvoorbeeld door middel van een aansprakelijkheidsbepaling in een verwerkerscontract. Juridisch heet een dergelijke clausule een exoneratie-beding. De AVG verbiedt een dergelijke beperking niet.

Kent de AVG hoofdelijke aansprakelijkheid en regresrecht?
Ja. Indien er namelijk meerdere verwerkingsverantwoordelijken of verwerkers bij dezelfde verwerking betrokken zijn, kan de betrokkene iedere verwerkingsverantwoordelijke of verwerker voor de volledige schade aanspreken. De verwerkingsverantwoordelijke en verwerker zijn onder de AVG dus hoofdelijk aansprakelijk. De AVG bepaalt voorts dat de aangesproken verwerkingsverantwoordelijke of verwerker een regresrecht heeft op de andere aansprakelijke verwerkingsverantwoordelijken of verwerkers.

Kent de AVG recht op schadevergoeding?
Artikel 82 van de AVG bepaalt dat de betrokkene recht heeft op schadevergoeding, indien zijn gegevens in strijd met de AVG worden verwerkt. Zowel materiële als immateriële schade komt daarbij voor vergoeding in aanmerking. De verwerkingsverantwoordelijke of de verwerker is enkel niet aansprakelijk, indien hij bewijst dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit.

Wie is aansprakelijkheid jegens de betrokkene onder de AVG?
De verwerkingsverantwoordelijke is aansprakelijk is voor de geleden schade van betrokkene. De verwerkingsverantwoordelijke is ook aansprakelijk, indien de gegevens feitelijk verwerkt worden door de verwerker. De verwerking geschiedt immers onder verantwoordelijkheid van de verwerkingsverantwoordelijke. De verwerker zelf is echter ook aansprakelijk. Die aansprakelijkheid strekt zich enkel uit tot ‘de schade die door verwerking is veroorzaakt wanneer bij de verwerking niet is voldaan aan de specifiek tot verwerkers gerichte verplichtingen van de AVG of indien buiten of in strijd met de rechtmatige instructies van de verwerkingsverantwoordelijke is gehandeld’.

Is het doorberekening van een boete van de AP toelaatbaar?
Ja, de doorberekening van bestuurlijke boetes van de AP wegens het niet melden van een datalek is een aanvullende afspraak die wel toelaatbaar is. Een bestuurlijke boete is namelijk schade die de verwerkingsverantwoordelijke lijdt als gevolg van het handelen (of nalaten) van de verwerker. Aangezien de AVG enkel ziet op de aansprakelijkheidsverdeling tussen verwerkingsverantwoordelijke en verwerker in relatie tot schade van de betrokkene, is het mogelijk om in de verwerkersovereenkomst afspraken te maken over schade die de verwerkingsverantwoordelijke lijdt als gevolg van het handelen van de verwerker.

Kan je je tegen de boetes verzekeren?

In Nederland is het wettelijk niet toegestaan een boete te verzekeren. Wel kun je de gevolgen van een boete of de gevolgen van een onrechtmatige verwerking verzekeren.

Kunt u de schade bij en de boete voor een datalek straks op uw IT-leverancier verhalen c.q. kunt u bij een beveiligingsinbreuk de daaruit voortvloeiende schadeposten verhalen op uw IT-leverancier??

De ernstigere datalekken/beveiligingsinbreuken moeten snel worden gemeld bij AP en/of de betrokkene. Dit kan met (hele) hoge kosten gepaard gaan. Onderzoek (laten) doen naar de details van een incident of een publiekscampagne opzetten is immers niet goedkoop. Bovendien bestaat de kans dat u een boete opgelegd krijgt, bijvoorbeeld omdat de melding niet snel genoeg is gedaan, of omdat uit de melding blijkt dat u uw beveiliging niet op orde had. Nu hebben veel organisaties hun IT al lang niet meer (volledig) intern in beheer.

Tekortkoming van leverancier vereist

De hoofdregel in de wet is overzichtelijk: de leverancier is verplicht de schade die voortvloeit uit een tekortkoming te vergoeden, tenzij de leverancier zich op overmacht kan beroepen (artikel 6:74 BW). Bij een tekortkoming kan de geleden schade dus in beginsel op de leverancier worden verhaald. Dat brengt ons direct bij de vraag: houdt een beveiligingsinbreuk ook een tekortkoming in? Dat hoeft niet per se zo te zijn. De vraag is waartoe de leverancier verplicht was. Immers, zonder verplichting geen tekortkoming.

Analyse van afspraken vereist

Er zal (dus) moeten worden gekeken in de contracten naar de verplichtingen die de leverancier op zich heeft genomen. Daarbij geldt grosso modo de volgende tweedeling:

1. Als er wel iets staat over de door de leverancier te verzorgen beveiliging(smaatregelen), dan moet worden getoetst of de leverancier die verplichtingen is nagekomen. Als dat niet het geval is, is in beginsel sprake van een tekortkoming;
2. Als er niets staat over de door de leverancier te verzorgen beveiliging(smaatregelen), dan is hoogstwaarschijnlijk de conclusie dat er ook geen sprake is van een tekortkoming. Weliswaar rust op IT-leveranciers een zorgplicht, maar die (algemene) zorgplicht gaat in de regel (doch niet altijd) niet zo ver dat hieruit een hele specifieke verplichting afgeleid kan worden tot het nemen van bepaalde maatregelen (zie bijv. recent nog het arrest van het Gerechtshof Amsterdam inzake Staalbouw).

Het laatste zou anders worden wanneer voor IT-leveranciers in de rechtspraak een bijzondere zorgplicht zou worden aanvaard, zoals die bijv. voor banken wel is aanvaard. Vooralsnog verwacht ik dat niet.

Analyse soms best een puzzel

De analyse van de gemaakte afspraken is soms best een puzzel. Vaak moeten meerdere documenten worden vergeleken en met elkaar in verband worden gebracht. Algemene voorwaarden willen hierbij nog wel eens een valkuil zijn.

Veel leveranciers nemen in hun voorwaarden namelijk uitdrukkelijk op dat ze niet gehouden zijn tot beveiliging, of slechts heel beperkt. Zo staat in artikel 7.1 van de Nederland ICT voorwaarden versie 2014 dat de leverancier er niet voor instaat dat de beveiliging onder alle omstandigheden doeltreffend is. Ook bepaalt artikel 6.2 dat de klant de leverancier moet vrijwaren voor aanspraken van personen van wie persoonsgegevens zijn geregistreerd. Die vrijwaring geldt alleen niet indien de klant bewijst dat de claims van die personen voortvloeien uit een fout van de leverancier. Dergelijke bepalingen nuanceren de verplichting van de leverancier dus al behoorlijk.

Niet ieder lek is ook een tekortkoming

Zelfs als er wel heel concrete afspraken zijn gemaakt over beveiliging, is het nog maar de vraag of er bij een datalek sprake is van een tekortkoming van de leverancier. Het kan immers best zijn dat de gemaakte afspraken prima zijn uitgevoerd, maar dat er toch een datalek heeft plaatsgevonden. De gemaakte afspraken kunnen bijv. te licht zijn gebleken (bijv. ingehaald door de tijd, of nooit actueel

geweest). Het kan ook zijn dat uw organisatie slachtoffer is van een zeer geraffineerde hack. In beide gevallen is de leverancier vermoedelijk niets te verwijten. Dat de gegevens feitelijk wel op straat liggen, doet daar niets aan af.

Aansprakelijkheid bovendien veelal (fors) beperkt

In bepaalde gevallen zal de conclusie echter zijn dat de leverancier wel degelijk een fout heeft gemaakt omdat hij een bepaalde concrete verplichting niet is nagekomen. Uitgangspunt van de wet is dan dat de volledige schade door de leverancier moet worden vergoed. De leverancier is dus bij een tekortkoming volgens de wet onbeperkt aansprakelijk. Daarbij moeten wel enkele algemene kanttekeningen in acht worden genomen, zoals dat schade die in een te ver verwijderd (causaal) verband staat buiten beschouwing wordt gelaten en dat wordt gecorrigeerd voor behaald voordeel en voor eigen schuld.

In de praktijk wordt echter bijna altijd van dit wettelijke uitgangspunt afgeweken. Bijna alle leveranciers hebben in de contracten (veelal forse) beperkingen van aansprakelijkheid opgenomen. In een zakelijke context zijn dergelijke contractsbepalingen in beginsel gewoon geldig. Dit betekent dat de schade die wordt geleden bij een beveiligingsinbreuk, alleen maar binnen de contractuele kaders (met beperking van aansprakelijkheid) kan worden verhaald.

Zo sluiten de Nederland ICT voorwaarden versie 2014 de aansprakelijkheid voor "verminking, vernietiging of verlies van gegevens of documenten" volledig uit. Verder wordt alleen aansprakelijkheid aanvaard voor directe schade (niet gedefinieerd) en komt schade van indirecte aard niet voor vergoeding in aanmerking. Onder de uitgesloten posten van indirecte aard vallen in ieder geval schade voor "bedrijfsstagnatie" en "schade als gevolg van aanspraken van afnemer". Onderaan de streep zal er onder de Nederland ICT voorwaarden vermoedelijk maar weinig schade voor vergoeding in aanmerking komen bij een aan de leverancier toe te rekenen beveiligingsinbreuk.

Dure les bij onvoldoende aandacht voor datalekken in contracten

Onvoldoende aandacht voor (de risico's van) datalekken in contracten kan uw organisatie dus duur komen te staan. Wat u niet afspreekt over beveiliging met uw leverancier, kunt u ook niet aan hem verwijten. En als u de leverancier al iets kunt verwijten, is nog maar de vraag of u dankzij de beperking van aansprakelijkheid iets van uw schade vergoed krijgt.

Het kan dus maar zo zijn dat de rekening voor een beveiligingsincident (bijna) volledig bij uzelf komt te liggen. Dat kan wel eens een (hele) dure les worden voor uw organisatie.

Kans op boetes

Sterker nog, het is niet ondenkbaar dat u bovenop de schade die u leidt bij een beveiligingsinbreuk, ook een boete opgelegd krijgt van de Autoriteit Persoonsgegevens. Een beveiligingsinbreuk kan er immers van getuigen dat:

- gegevens voor een doeleinde zijn verwerkt dat niet met het verzameldoel is te verenigen;
- gegevens langer zijn bewaard dan noodzakelijk;
- onvoldoende maatregelen zijn getroffen om de relevantie van gegevens te borgen
- onvoldoende maatregelen zijn getroffen om de juistheid van gegevens te borgen;
- niet geborgd is dat de personen die persoonsgegevens verwerken tot geheimhouding verplicht zijn;
- onvoldoende passende beveiligingsmaatregelen getroffen zijn;
- persoonsgegevens voor doeleinden zijn verwerkt waarover de betrokkene niet is geïnformeerd.

Op iedere overtreding van de AVG staat een boete. Voor die boete is wel vereist dat de overtreding opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid. Wat precies onder die opzet en ernstig verwijtbare nalatigheid moet worden verstaan is vooralsnog niet geheel duidelijk. Uit de wetgeschiedenis blijkt wel dat de opzet niet gericht hoeft te zijn geweest op overtreding van de wet. Dat betekent dat het verweer "Ik had niet de bedoeling de AVG te overtreden" op zichzelf in ieder geval niet voldoende is om onder een boete uit te komen.

Weliswaar staat op het niet sluiten van een (adequate) verwerkersovereenkomst geen .Dat neemt echter niet weg dat de Autoriteit Persoonsgegevens wel zou kunnen stellen dat de slechte afspraken er toe leiden dat niet is geborgd dat persoonsgegevens "op behoorlijke en zorgvuldige wijze verwerkt" worden als bedoeld in AVG, noch dat deze goed beveiligd zijn als bedoeld in AVG.
Kritisch inkopen vereist
Het voorgaande bevestigt eens te meer dat het van belang is bij de inkoop van IT-dienstverlening kritisch te kijken naar

1. De risico's die zich kunnen voordoen; en
2. In hoeverre de dienstverlening en de toepasselijke contractuele voorwaarden aansluiten op die risico's.

Meld- en administratieplicht beveiligingsinbreuken bredere consequenties heeft dan alleen de meld- en administratieplicht als zodanig. Om goed aan deze nieuwe verplichtingen te kunnen voldoen, zonder dat het de organisatie (heel) veel pijn kost, is kritisch inkopen vereist. Het zal interessant zijn om te zien of dat ook gaat gebeuren en zo ja, in hoeverre leveranciers nog lang weg zullen komen met (de thans gebruikelijke) beperkingen van aansprakelijkheid die er in feite op neer komen dat schade niet tot nauwelijks op leveranciers is te verhalen.
Verder is van het belang in de organisatie ook andere maatregelen te treffen om de risico's te dempen, zoals het sluiten van adequate verzekeringen. Mocht dat niet gebeuren, dan over enige tijd zaken voorbij gaan zien komen over bestuurdersaansprakelijkheid vanwege het onvoldoende borgen van privacy risico’s. Vanuit juridisch perspectief interessante ontwikkelingen.

122. Beleidsregels. Accountability

Wat zegt de AP over Accountability?
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verantwoordingsplicht?qa=accountability

Hoe pak je accountability voor AVG aan?
Een organisatie (verwerkingsverantwoordelijke of verwerker), maar zeker ook leidinggevenden moeten ervoor zorgdragen dat de vereisten van de AVG aantoonbaar worden nagekomen. Alleen dan kan een organisatie accountable zijn. Dit vereist een administratie die 'evidence based' is ingericht. Dat is belangrijk en nodig omdat de AVG een omgekeerde bewijslast kent. Hieronder volgt een methodiek voor een aanpak:

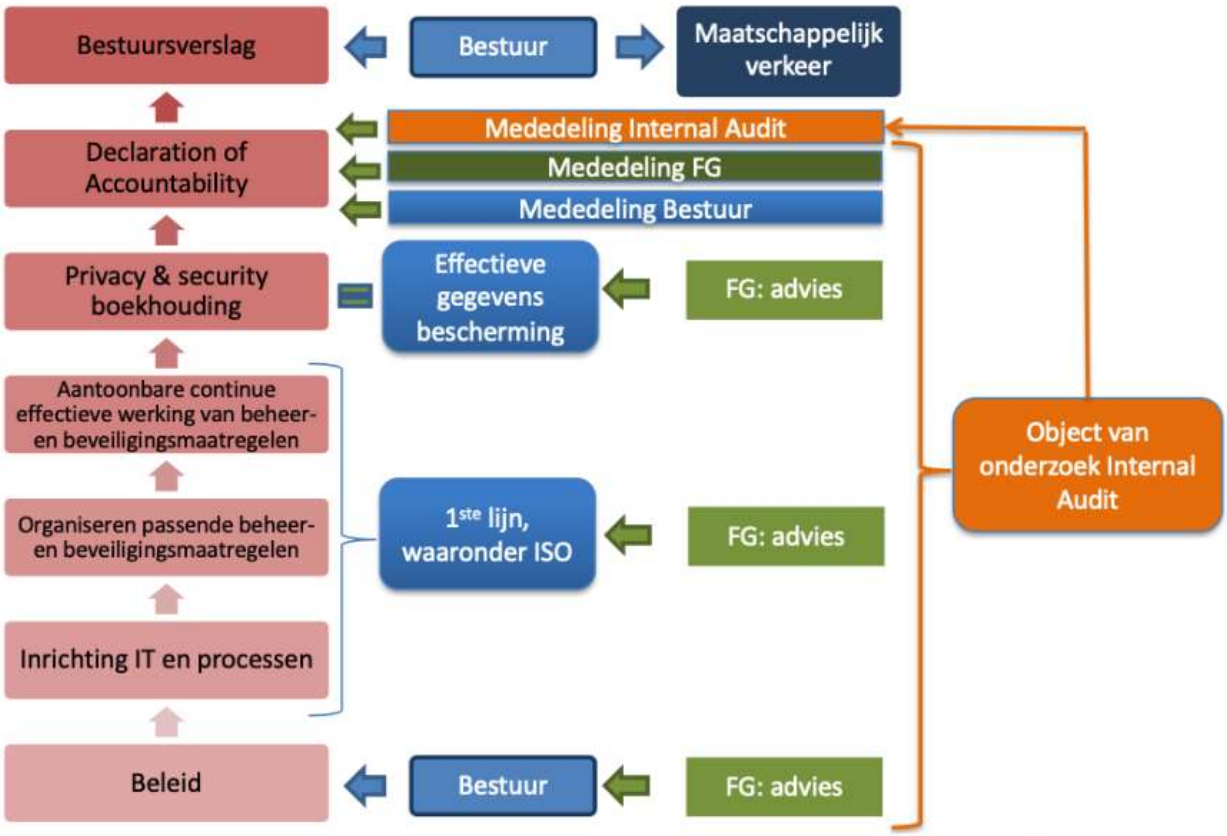
- De basis is een normenkader dat gebaseerd is op de AVG, aanpalende en sectorale wetgeving, en de hieruit afgeleide baseline waarin de passende technische en organisatorische maatregelen zijn beschreven. Deze baseline kan nog verder aangevuld worden met normen van de eigen organisatie.
- Dat is simpel geschreven maar een hele kluif om dat te bereiken. Een goed opgeleide FG is hierbij nodig alsook vaak (externe) juridische hulp. Gelukkig hoeft niet alles zelf ontwikkeld te worden, er zijn sectorale normenkaders en baselines beschikbaar in de markt waarop een abonnement genomen kan worden.
- Maar dan zijn we er nog niet. Er zal moeten worden aangetoond dat minimaal aan de baseline wordt voldaan. Hiervoor is een privacy administratie nodig waaruit moet blijken dat de technische en organisatorische maatregelen effectief hebben gewerkt. Deze administratie heeft weer input nodig vanuit de security administratie, de registers, de ketenpartners enz. Om aan de omgekeerde bewijslast te kunnen voldoen zal op elk moment de werking van de maatregelen aangetoond moeten kunnen worden. Dat is op dit moment voor veel organisaties niet haalbaar. In het verleden zijn systemen gebouwd waarin controleerbaarheid niet als deliverable is meegenomen. Maar ook bij het opzetten van operationele processen is controleerbaarheid niet meegenomen. Niet alleen bij de organisatie zelf kan dit niet op orde zijn maar ook bij een of meerdere ketenpartners. Dit maakt dat organisaties (of zelfs een hele keten) niet of niet geheel kunnen voldoen aan de vereisten van de Avg.

Wat is een Declaration of Accountability voor persoonsgegevens?
Het is een inherente verantwoordelijkheid van een onderneming om zich te verantwoorden over de bescherming van persoonsgegevens. Duthler Associates noemt een dergelijk verantwoordingsverslag een 'Declaration of Accountability', afgekort een DoA. Duthler motiveert ondernemingen om deze verantwoording op te stellen en in verkorte vorm op te nemen in het bestuursverslag.

Waaruit bestaat de Declaration of Accountability?
De DoA bestaat uit diverse onderdelen waaruit blijkt welke persoonsgegevens de organisatie verwerkt en hoe deze gegevens beschermd worden. Ook zijn drie verklaringen opgenomen. De eerste is van het bestuur waarin het behaalde volwassenheidsniveau wordt toegelicht en de ambities voor de komende jaren wordt uiteengezet. De tweede verklaring is van de FG. De FG heeft onder andere als wettelijke taak het toezien op de naleving van de AVG en heeft in deze verklaring de mogelijkheid om hiervan verslag te doen. De derde verklaring is van de interne controleur die vaststelt of het door de leiding voorgestelde niveau van bescherming van persoonsgegevens aantoonbaar ondersteund kan worden.

https://duthler.nl/2019/05/02/privacyverantwoording-livit-laat-zien-waarom-en-hoe/

Hoe kun je de workflow van een DoA weergeven?



Bron: https://duthler.nl/2018/11/01/white-paper-declaration-of-accountability-doa/

123. Beleidsregels. Boete

Wat zegt de Autoriteit Persoonsgegevens over boete?
Beleidsregels van de Autoriteit Persoonsgegevens van 19 februari 2019 met betrekking tot het bepalen van de hoogte van bestuurlijke boetes (Boetebeleidsregels Autoriteit Persoonsgegevens 2019)
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-14586.pdf

Wat zeggen anderen over boete?
https://ploum.nl/uploads/documents/Drie_jaar_AVG-boetes_wat_zijn_de_lessons_learned_(NW_en_LB).pdf?utm_medium=email

Waarvoor kan de Autoriteit Persoonsgegevens boetes opleggen?
De AP kan boetes opleggen bij overtredingen van de Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet van de AVG. De AP kan ook bij overtredingen op grond van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens een boete opleggen en bij bepaalde overtredingen van de Telecommunicatiewet, de eIDAS-verordening en de Algemene wet bestuursrecht.

Wat is de aansprakelijkheid naar een individuele burger onder de AVG?
Kenmerkend voor de aansprakelijkheid tegenover een burger is dat die niet valt uit te sluiten of te beperken. Degene die de AVG schendt moet in beginsel voor de volle schade van de burger opdraaien. Van dat uitgangspunt kan in een contract met de burger niet worden afgeweken. De rechter mag de reputatieschade overigens schatten.

Kan de Autoriteit Persoonsgegevens (AP) een persoonlijke boete opleggen aan de bestuurder(s) van een onderneming, net als de ACM onder de Mededingingswet?
Ja, onder meer bij het niet melden van een datalek wanneer dit wel verplicht was, loopt de bestuurder het risico om persoonlijk aansprakelijk te worden gesteld. Uit de Parlementaire Geschiedenis blijkt dat deze boete ook aan natuurlijke personen kan worden opgelegd indien: "*zij feitelijk leiding hebben gegeven respectievelijk opdracht hebben gegeven tot het verrichten van de verboden gedraging en hebben nagelaten om maatregelen te treffen ter voorkoming van een verboden gedraging en daarmee bewust de kans wordt aanvaard dat deze gedraging zal plaatsvinden.*" De persoonlijke boete zal waarschijnlijk bovenop de boete komen die aan de onderneming wordt opgelegd. Wanneer de AP besluit om een boete op te leggen dient het boetebedrag te worden vastgesteld aan de hand van de aard, de ernst en de duur van de inbreuk, of de inbreuk opzettelijk of nalatig van aard was en welke maatregelen zijn getroffen door de verwerkingsverantwoordelijke of de verwerker om de door betrokkenen geleden schade te beperken. De wetgever heeft hierover wel al aangegeven dat er een zwaardere bewijslast bestaat.

Kan een bestuurder ook persoonlijk worden aangesproken door betrokkenen van wie er gegevens gelekt zijn?
Ja, de Uitvoeringswet AVG (UAVG) bepaalt dat de bestuurders van een verwerkingsverantwoordelijke alsmede van de verwerker in persoon aansprakelijk kunnen worden gesteld in het geval iemand schade lijdt doordat er in strijd wordt gehandeld met de AVG. Deze persoonlijke aansprakelijkheid kan men ook via de gewone civiele wijze bewerkstelligen, zoals bijvoorbeeld aansprakelijkstelling van de bestuurder voor onrechtmatige daad. De wet geeft ook aan dat een bestuurder zijn taken goed moet vervullen. Een bestuurder kan aansprakelijk worden gesteld als er sprake is van onbehoorlijk bestuur en de bestuurder een ernstig verwijt kan worden

gemaakt. Daarnaast moet er sprake zijn van schade. In de wet is ook een regeling opgenomen over de interne aansprakelijkheid van de bestuurder jegens de rechtspersoon. De rechtspersoon spreekt dan de bestuurder aan als er een boete is opgelegd aan de rechtspersoon.

Een derde (de betrokkene) kan een aanspraak doen op de externe aansprakelijkheid van artikel 6:162 BW. er moet dan sprake zijn van onzorgvuldig handelen, waardoor de betrokkene schade heeft geleden.

Hoe vaak een boete?
AP tot juli 2021 in totaal 15 boetes. Daarvan 1 door rechter gematigd en 1 vernietigd.

Waarvoor boete?
Vier clusters:

- Melden van een datalek (AVG 2.1)
- Beveiliging van persoonsgegevens (AVG 2.2)
- Rechtmatigheid van de verwerking (AVG 2.3)
- Rechten van betrokkenen en de informatieverplichting (AVG 2.4)

124. Beleidsregels. KVK Handelsregister en Persoonsgegevens

Wat zegt de Autoriteit Persoonsgegevens over Kvk?
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brf.-kvk-20dec18-handelsregisterinfoproducten.pdf

Wat zegt KvK over AVG en persoonsgegevens?
https://www.kvk.nl/privacy/privacy-en-het-handelsregister/
https://www.kvk.nl/inschrijven-en-wijzigen/inschrijven-bij-de-kamer-van-koophandel/uw-gegevens-in-het-handelsregister/prive-adres-in-het-handelsregister/

Wat is de positie van het Handelsregister binnen de AVG
Het Handelsregister heeft een uitzonderingspositie binnen de AVG omdat het een openbaar register betreft.

Van welke personen staan er gegevens in het Handelsregister?
In het Handelsregister staan de gegevens van natuurlijke personen met een onderneming (eenmanszaken, vof's en maatschappen) en van functionarissen van rechtspersonen (denk aan bestuurders).

Welke gegevens van personen worden opgenomen in het Handelsregister?
Bij eenmanszaken (zzp'ers), vof's en maatschappen zijn dit de persoonsnaam, privéadres, geboortedatum, geboorteplaats en datum overlijden. Daarnaast staan er ook gegevens in die indirect te herleiden zijn tot een persoon. Hierbij kun je denken aan het KVK-nummer, de handelsnaam (als daarin is verwerkt de naam van de eigenaar), het vestigingsadres (als dit gelijk is aan het woonadres), een (mobiel) telefoonnummer en mogelijk het e-mailadres.
Verder worden er ook van functionarissen van een rechtspersoon gegevens opgenomen die gezien worden als persoonsgegevens. Dit zijn het privéadres, (mobiele) telefoonnummer, en de geboortedatum/-plaats. Let op: de gegevens van rechtspersonen zelf (denk bijvoorbeeld aan bv's, nv's) worden niet gezien als persoonsgegevens. Een voorbeeld: **van de rechtspersoon** Klusbedrijf Jansen BV, **zijn het KVK-nummer, de handelsnaam, het vestigingsadres, telefoonnummer en e-mail geen persoonsgegevens. Ook niet als het vestigingsadres het privéadres** van de heer Jansen **is en het telefoonnummer van de onderneming gelijk is aan zijn eigen mobiele nummer**.

Welke persoonsgegevens in het Handelsregister zijn openbaar?
Dit zijn: naam, adres, geboortedatum, geboorteplaats, datum van overlijden

Welke persoonsgegevens in het Handelsregister zijn niet openbaar?
Dit zijn onder andere: burgerservicenummer, handtekening, geslacht, privéadres functionaris rechtspersoon

Op welke gegevens uit het Handelsregister is de AVG van toepassing?
De AVG is alleen van toepassing op de gegevens in het Handelsregister die gezien worden als persoonsgegevens (zoals hierboven omschreven). Het gaat dus om de gegevens van natuurlijke personen met een onderneming (zoals eenmanszaken, vof's en maatschappen) die te herleiden zijn naar een natuurlijke persoon en gegevens van functionarissen van rechtspersonen.
Let op: de AVG beschermt weliswaar de privacy van personen maar er is een uitzondering gemaakt voor bij wet ingestelde openbare registers, zoals het Handelsregister. Dat betekent dat de AVG van toepassing is op het Handelsregister, maar dat KVK op basis van de Handelsregisterwet een

grondslag heeft om de gegevens te verwerken voor haar wettelijke taken (zoals beschreven in de in artikel 2 van de Handelsregisterwet aangegeven doelen). Dat betekent dat de persoonsgegevens die in het Handelsregister openbaar zijn (zoals naam, adres), ook na 25 mei 2018 openbaar zijn en blijven. Verder betekent dit ook dat als je ben ingeschreven in het Handelsregister je een aantal rechten niet hebt. Zo kun je onder andere niet verzoeken om je gegevens uit het Handelsregister te laten verwijderen (het zogenaamde recht om vergeten te worden) of bezwaar maken tegen de verwerking van je gegevens in het Handelsregister.

Verandert er door de AVG iets aan de openbaarheid van de gegevensverstrekking uit het Handelsregister?
Nee, door de AVG verandert er niets aan de openbaarheid van het Handelsregister. De AVG beschermt weliswaar de privacy van persoonsgegevens maar er is een uitzondering gemaakt voor bij wet ingestelde openbare registers, zoals het Handelsregister. Dat betekent dat de AVG van toepassing is op het Handelsregister, maar dat KVK op basis van de Handelsregisterwet een grondslag heeft om de gegevens te verwerken voor haar wettelijke taken (zoals beschreven in de in artikel 2 van de Handelsregisterwet aangegeven doelen).

Waarom is een privéadres soms openbaar in het Handelsregister?
In sommige gevallen is een privéadres openbaar in het Handelsregister. Dat is afhankelijk van de rechtsvorm. Als je eigenaar bent van een eenmanszaak, vof of maatschap (ondernemingsvormen die door veel zzp'ers worden gebruikt) is je privéadres openbaar. Bij deze ondernemingsvormen is zowel het vestigingsadres van de onderneming als het privéadres van de eigenaar zichtbaar. De reden hiervoor is dat de eigenaar persoonlijk aansprakelijk is voor de onderneming en fysiek traceerbaar moet zijn. Dit zorgt voor (rechts)zekerheid waardoor ondernemers in Nederland het vertrouwen hebben om met elkaar zaken te doen.
In het geval van een waarschijnlijke dreiging, is het in bepaalde situaties mogelijk je privéadres in het Handelsregister af te schermen via een verzoek aan KVK. Hiervoor moet je wel al zelf maatregelen genomen hebben om de bekendheid van je adres te verminderen. Bij toewijzing van het verzoek is je privéadres niet langer openbaar, maar alleen nog in te zien door speciaal daartoe gerechtigde organisaties zoals bestuursorganen, deurwaarders, advocaten en notarissen.

In het Handelsregister staan persoonsgegevens van onze bestuurders (van onze stichting, vereniging etc.). Is KVK dan een verwerker van onze persoonsgegevens en is er dan een verwerkersovereenkomst nodig?
Nee, KVK verwerkt op grond van de Handelsregisterwet de (persoons)gegevens van ondernemers en functionarissen van rechtspersonen in het Handelsregister. Op grond van de privacywetgeving en de Handelsregisterwet is KVK verwerkingsverantwoordelijke. Hierdoor is het sluiten van een verwerkersovereenkomst (met ondernemingen die in het Handelsregister zijn opgenomen) niet van toepassing.

Ik heb geen toestemming gegeven om mijn adres te verkopen, stoppen jullie daar nu mee?
Wij begrijpen dat het vervelend is dat inschrijving in het Handelsregister kan leiden tot ongewenste marketing. Wij zijn verplicht om gegevens uit het Handelsregister te leveren als hier om gevraagd wordt. Dit is opgenomen in de Handelsregisterwet. Dus kunnen we niet zomaar stoppen met het leveren van jouw gegevens. Wel moet de afnemer zich houden aan de geldende privacywetgeving en indien aangegeven de wens van ondernemers respecteren niet met direct marketing geconfronteerd willen worden.
Privacy waarborgen bij de UBO?
Vanaf januari 2020 treedt het UBO-register in Nederland in werking (implementatie richtlijn EU 2015/849). Ondernemingen en rechtspersonen zijn vanaf 2020 verplicht om hun uiteindelijk

belanghebbenden, ofwel UBO's (ultimate beneficial owners) te registreren. Met andere woorden: wie uiteindelijk de belanghebbende en/of de beleidsbepaler is binnen de organisatie. Met "wie" wordt dan een natuurlijk persoon bedoeld die uiteindelijk een aandelenbelang heeft van meer dan 25%. Dus als een onderneming formeel door een andere onderneming bestuurd wordt (zoals het geval is in concernrelaties), dan dient het handelsregister te vermelden welke natuurlijke persoon leiding geeft aan de besturende onderneming.Doel van het register is het tegengaan van financieel-economische criminaliteit, zoals witwassen van geld en terrorismefinanciering door transparantie over wie de uiteindelijk belanghebbende van een onderneming is.
Een deel van de persoonsgegevens van de UBO zoals diens naam en economisch belang wordt via het register openbaar. Het openbare deel van het UBO-register is echter alleen doorzoekbaar op naam van de onderneming of rechtspersoon. Zoeken op naam van de UBO is dus niet mogelijk. Daarnaast is er nog een extra drempel ingebouwd; het opvragen van de gegevens uit het register kost geld.
Het register voldoet aan de eisen voor gegevensbescherming en de Algemene Verordening Gegevensbescherming (AVG). In uitzonderlijke omstandigheden kan een UBO verzoeken de openbare gegevens af te laten schermen. Bijvoorbeeld wanneer er sprake is van een onevenredig risico op kidnapping of geweld. Instanties zoals het Openbaar Ministerie, de politie, de Belastingdienst en de Financiële Inlichtingen Eenheid kunnen wel altijd deze gegevens inzien.

Conflict tussen AVG en UBO-registratieplicht?
Nee, artikel 6 lid 1 sub c van de AVG bepaalt immers dat persoonsgegevens verwerkt (onder verwerking valt ook registreren en publiceren) mogen worden, indien dit gedaan wordt op basis van een wettelijke verplichting. Door wetgeving bestaat er voor organisaties en voor de Kamer van Koophandel een wettelijke verplichting om de persoonsgegevens van de UBO te registreren/publiceren, en wordt dus voldaan aan het vereiste uit de AVG.

125. Beleidsregels. Openbaarmaking Autoriteit Persoonsgegevens

Wat zegt de Autoriteit Persoonsgegevens over Openbaarmaking?
https://autoriteitpersoonsgegevens.nl/nl/nieuws/nieuwe-beleidsregels-actieve-openbaarmaking-autoriteit-persoonsgegevens

Is openbaarmaking door AP wettelijk vastgelegd?
Ja, zie Beleidsregels openbaarmaking door de Autoriteit Persoonsgegevens
https://wetten.overheid.nl/BWBR0037531/2016-01-13

Welke gegevens maakt de AP openbaar?
De Autoriteit Persoonsgegevens neemt alle meldingen van datalekken op in een register. Dit register is niet openbaar. De Autoriteit Persoonsgegevens kan wel een onderzoek starten naar aanleiding van een gemeld lek, waarbij er in dat kader wel bedrijfsnamen en namen van verantwoordelijken van de (rechts)persoon kunnen worden gepubliceerd. Er wordt hierbij wel een uitzondering gemaakt voor bedrijven waarvan de naam van een natuurlijk persoon deel uitmaakt van de bedrijfsnaam: in dat geval wordt de bedrijfsnaam in beginsel niet gepubliceerd. Daarnaast houdt de Autoriteit Persoonsgegevens rekening met zwaarwegende gronden die voor een publicatie in de weg staan.

126. Beleidsregels. Diensten Whatsapp, WeTransfer, Snapchat en Dropbox

Wat zegt de Autoriteit Persoonsgegevens over digitale diensten in de cloud?
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/praktijkgids_patientgegevens_in_de_cloud_def.pdf

Wat voor soorten diensten?

- E-maildiensten o.a. Google Gmail
- Clouddiensten o.a. Microsoft OneDrive / Office 365, Google G Suite / Google Drive en Apple ICloud, Dropbox
- Social Media o.a. Facebook en Twitter
- Berichtendiensten o.a. WhatsApp
- Dataverzendingsdiensten o.a. WeTransfer

Wat zijn de MAAS alternatieven?

- E-maildiensten – MAAS Outlook
- Clouddiensten – SAP systeem, CRM systeem,
- Social Media – Marketing
- Berichtendiensten – MAAS Outlook
- Dataverzendingsdiensten – concept versie MAAS Portal https://maasportal.maas.nl/

Hoe is ervoor gezorgd dat de MAAS websites AVG-proof zijn?
Om aan de regels van de AVG te voldoen, heeft de website minimaal een SSL certificaat en een privacy verklaring.

Zijn websites herkenbaar als MAAS met een geldig MAAS SSL certificaat?
Het betreft:

- MAAS portal https://maasportal.maas.nl/ : DNS name *.maas.nl
- MAAS Website https://maas.nl/: DNS name *.maas.nl
- MAAS Webshop https://webshop.maas.nl/customer/account/login/ DNS name webshop.maas.nl
- MAAS Intranet

Is het veilig om bestanden te delen via Dropbox of WeTransfer?
Dat ligt er aan welke informatie de bestanden bevatten. Als het bijvoorbeeld om een dossier, een jaarrekening, een eigendomsbewijs of een salarisstrook gaat, dan is dat zeker niet aan te raden. Omdat van deze partijen niet duidelijk is waar de bestanden precies staan (binnen of buiten de EU) en op welke manier de beveiliging geregeld is. Verstuur je de opmaak van een pagina uit een reisgids, dan is het weer geen probleem. Wil je toch privacygevoelige gegevens uitwisselen? Dan is een gesloten systeem de beste optie. Binnen zo'n besloten netwerk kan je veilig gegevens uitwisselen.

Wat is een goed alternatief voor WeTransfer?
Het delen van grote bestanden kan in veel gevallen ook niet via e-mail. En als het wel kan via e-mail, is het ook de vraag of dat veilig is. Wat je dan wel kunt gebruiken als goed alternatief voor WeTransfer? Zivver is een beveiligde verzendmethode voor het versturen van (grote) bestanden. Een ander alternatief voor WeTransfer is FileCap. Deze partij voldoet, net als Zivver, aan de AVG.

Waarom is WhatsApp niet geschikt voor zakelijk gebruik?
Een voorbeeld is de manier waarop de applicatie je contacten inlaadt. Wanneer je WhatsApp op je telefoon installeert, moet je de app toestemming geven om al je contacten (op je toestel) te kunnen inzien en gebruiken. Veel mensen hebben WhatsApp geïnstalleerd op hun privémobieltje, maar ook op hun zakelijke. Jij deelt dus als het ware de gegevens van je contacten met WhatsApp. Hier moet je dus voorzichtig mee zijn, want jouw contacten hebben je misschien niet eens toestemming gegeven voor het delen van hun gegevens met een derde partij toen zij jou hun telefoonnummer gaven. MAAS moet kunnen aantonen dat zij toestemming hebben gekregen van hun klanten om hun gegevens te bewaren. Iets dat onmogelijk is als WhatsApp automatisch alle gegevens uit je contactlijst inleest en gebruikt.

Voldoet WhatsApp aan de AVG (Europese Privacywetgeving)?
Nee. De redenen zijn:

1. Het adresboek van de gebruiker inclusief e-mailadressen en telefoonnummers worden naar WhatsApp en dus Facebook overgebracht. Het is onduidelijk waarom en voor welk doel deze gegevens worden overgedragen en verwerkt. Dit is echter wel een eis. MAAS kan hierdoor klanten, medewerkers en anderen niet informeren over de manier waarop deze gegevens worden verwerkt. Automatisch voldoet MAAS niet aan de AVG vereiste “recht op toegang”. Klanten, medewerkers en andere gebruikers kunnen hierdoor namelijk niet gebruik maken van “recht om te worden vergeten” om zodoende al zijn/haar gegevens uit WhatsApp te verwijderen.
2. MAAS heeft geen uitdrukkelijke toestemming om de persoonlijke gegevens van klanten, medewerkers en andere gebruikers over te dragen aan WhatsApp. Als WhatsApp wordt gebruikt verzendt MAAS het adresboek naar WhatsApp en dus ook de contactgegevens van WhatsApp.
3. Door WhatsApp voor zakelijke doeleinden te gebruiken, draagt MAAS klantgegevens over naar de VS. Dit is in strijd met de verplichting van de AVG om geen persoonlijke gegevens buiten de EU over te dragen of op te slaan. In de VS met zijn zwakkere privacywetgeving kan een adequate bescherming van klantgegevens niet worden gegarandeerd.
4. Het is onwaarschijnlijk dat WhatsApp voldoet aan de beginselen van 'privacy by design' en ‘anonimiseren’. De verbinding voor het uploaden en opslaan van het adresboek voldoet niet aan het concept 'privacy by design'. Vanwege het onderliggende advertentiebedrijfsmodel van Facebook is het onwaarschijnlijk dat het anonimiseren op grote schaal wordt toegepast.
5. Als MAAS alle gegevens van een klant naar een andere service moet overzetten, is dit niet mogelijk met WhatsApp. De persoonlijke gegevens van een klant zijn eigenlijk geblokkeerd in WhatsApp. Dus met betrekking tot de "dataportabiliteit" van de AVG zijn bedrijven niet-conform als ze WhatsApp gebruiken.

Wat dien je bij MAAS te gebruiken als alternatief voor Whatsapp?
Het versturen van via een gesloten netwerk: Maas email

Is het veilig om bestanden te delen via Dropbox of WeTransfer?
Nee, omdat van deze partijen niet duidelijk is waar de bestanden precies staan (binnen of buiten de EU) en op welke manier de beveiliging geregeld is.

- Dropbox vereist van niet-Amerikaanse overheden dat deze samenwerken met Amerikaanse overheidsinstanties, zodat een Amerikaanse rechtbank de vereiste juridische procedure kan opleggen aan Dropbox (https://www.dropbox.com/transparency).
- WhatsApp Inc. deelt gegevens wereldwijd, zowel intern met de Facebook-bedrijven als extern met bedrijven, serviceproviders en partners en met diegenen wereldwijd waarmee je

communiceert en gegevens deelt. Je gegevens kunnen bijvoorbeeld worden doorgegeven aan of verzonden naar, of worden opgeslagen en verwerkt in de Verenigde Staten of andere landen waar je niet woont, voor de doeleinden die in Whatsapp Privacybeleid worden beschreven https://www.whatsapp.com/legal/?eea=1#privacy-policy-how-you-exercise-your-rights

Hoe zou je WhatsApp AVG-proof kunnen inzetten?

1. Wil je een toestel gebruiken, gebruik dan een leeg toestel, waarin je enkel op basis van opt-in de contacten vastlegt van personen die zelf met jou willen communiceren op WhatsApp. Daarnaast moet je dan een procedure hebben die in lijn is met MAAS Privacy beleid en je bewaartermijn van gegevens, waarbij je dus regelmatig de contacten en conversaties in het toestel verwijdert op basis van je beleid.
2. Gebruik een messaging applicatie die WhatsApp kan ondersteunen en waarin je de bewaartermijn van gegevens volledig AVG proof kunt instellen. Dan komt er geen toestel aan te pas en worden er geen contactlijsten gedeeld en worden persoonsgegevens automatisch gewist.

Wil je – zonder WhatsApp, Dropbox of We Transfer - toch privacygevoelige gegevens uitwisselen?
Dan is een gesloten systeem, zoals MAAS netwerk, de beste optie. Binnen het MAAS netwerk kan je veilig gegevens uitwisselen.

Welke benchmark?
Het advies van de KNMG is WhatsApp alléén te gebruiken voor het versturen van patiëntinformatie wanneer dit de zorg voor de patiënt aantoonbaar ten goede komt én geen tot de persoon herleidbare gegevens uit te wisselen via de app. De KNMG raadt aan foto's zowel bij de verzender als de ontvanger te wissen. Blijken de gegevens wel tot een patiënt te herleiden, dan is het veiliger om andere communicatiemiddelen te gebruiken, bijvoorbeeld beveiligde e-mail. Het is aan het veld dit advies uit te werken in richtlijnen. Veel ziekenhuizen hebben wel richtlijnen voor het gebruik van sociale media, maar meestal niet specifiek voor WhatsApp.

127. AVG en USA Cloud Act

Wat is de Cloud Act?
De CLOUD Act is een wet waarbij CLOUD een acroniem is die staat voor 'Clarifying Lawfull Oversees Use of Data'. Deze aanpassing geldt in hoofdzaak voor een wet uit 1986 die als verouderd gezien werd, de zogenaamde Stored Communications Act (SCA). Hiervan vonden velen dat deze wet niet ver genoeg ging, omdat deze in hoofdzaak handelt over data die buiten de Verenigde Staten wordt opgeslagen. De SCA omvat tevens een procedure waarin de mogelijkheid aan providers wordt gegeven om een dataverzoek vanuit de overheid aan te vechten. Uitgerekend deze SCA is momenteel de wet waarover Microsoft met de Amerikaanse overheid een dispuut heeft. De CLOUD Act vormt een aanvulling op de SCA en moet deze procedure-mogelijkheden gaan beperken.

Waar gaat de CLOUD Act over?
De CLOUD Act bepaalt dat Amerikaanse providers de verplichting krijgen om data van betrokkenen af te staan aan de Amerikaanse justitie, waar deze ook ter wereld opgeslagen zijn. Aanvullend geldt dat dit niet alleen op verzoek van de Amerikaanse overheid hoeft te zijn, maar dat ook andere landen een verzoek daartoe kunnen richten aan Amerikaanse providers.
De tekst uit de CLOUD Act, Paragraaf 2713 luidt:
'*Electronic communication service providers and remote computing service providers must comply with the obligations of (the SCA) to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States'.*
In de afgelopen jaren waren er cases waarbij instanties zoals de FBI moeite hadden om toegang te krijgen tot gegevens die op computers in andere landen waren opgeslagen. De CLOUD-wet vereist dat Amerikaanse bedrijven toegang verlenen tot dergelijke gegevens, ongeacht in welk land het bedrijf het opslaat. Met de huidige case van Microsoft als slepend voorbeeld. Ook de dataverzoeken die aan andere landen gedaan worden, moeten nog door bilaterale verdragen middels de Mutual Legal Assistance Treaty (MLAT) afgehandeld worden. Ook dit werd als een inefficiënt en tijdrovend proces gezien.

Wat is er mis met de CLOUD Act?
Alleen een 'Qualifying foreign government' kan toegang krijgen tot gegevens die zich in de Verenigde Staten bevinden. Als een land deze kwalificatie niet bezit, dan kan de Amerikaanse Attorney General dit kwalificatiezegel op verzoek en na gedegen onderzoek afgeven aan het betreffende land. De EU en haar lidstaten bezit dit kwalificatiezegel niet en uiteraard geldt dit zegel uitsluitend voor individuele landen, wat inhoudt dat ieder Europees land individueel door deze kwalificatiemolen heen zal moeten. Het geeft ook meer macht inzake besluiten tot openbaarheid van in de Verenigde Staten opgeslagen data aan een paar mensen in plaats van gekwalificeerde instanties en een onafhankelijke rechter.

Welke botsing met de AVG?
De CLOUD Act botst met de AVG op artikel 48 van laatstgenoemde. Dit artikel bepaalt dat data uitsluitend met niet-Europese landen uitgewisseld mag worden op basis van een gerechtelijke uitspraak die gebaseerd is op een bilateraal verdrag (zoals de MLAT). Zonder de vermelde uitzonderingsgevallen kan en zal geen gehoor worden gegeven aan een data-uitwisselings-verzoek.

De CLOUD Act is geen overeenkomst die met de EU als geheel kan worden afgesloten, maar moet met ieder land afzonderlijk.

Deze verdragen bestaan momenteel (nog) niet. Daarmee lijkt het dat beide wetten niet naast elkaar kunnen leven.
Met het van kracht worden van de CLOUD Act is de rol van verdragen (MLAT) uitgespeeld. Artikel 48 AVG kan als gevolg daarvan geen toepassing meer vinden. Dan kan er nog gekeken worden naar artikel 49 AVG, lid 1 sub d en lid 1 slot. In deze beide gevallen dient een afweging van belangen gemaakt te worden. De CLOUD Act biedt echter geen ruimte voor een dergelijke belangenafweging, waarmee de verhoudingen op scherp komen te staan.

Waar gaat het mis?
De CLOUD Act betekent dat Amerikaanse providers, al dan niet met datacenters op Europees grondgebied, die geconfronteerd worden met een beslissing dat zij data moeten openbaren die zich in de EU bevinden, geen mogelijkheid meer hebben om die beslissing aan te vechten. Zij zullen daaraan moeten voldoen. Tegelijkertijd betekent het voldoen aan zo'n beslissing echter ook dat deze provider in strijd handelt met zijn verplichtingen onder de AVG/GDPR en daardoor zeer hoge boetes riskeert.

X MYTH: The CLOUD Act enables widespread access to EU citizens' data, effecting the return of US bulk surveillance.
✓FACT: The CLOUD Act does not authorize bulk surveillance, and only applies to court-authorized criminal investigations.
The CLOUD Act does not authorize bulk requests by law enforcement. Instead, law enforcement may only access digital content from service providers:
1. in connection with a criminal case;
2. after obtaining a warrant from a court based on probable cause; and
3. only the specific types of data that are identified with particularity in the warrant itself.

https://www.bsa.org/files/policy-filings/02282019CLOUDACTEUMythvsFact.pdf

128. Milieu. Ongewoon voorval

Wat zegt de AP over een ongewoon voorval milieu?
Geen specifieke informatie

Bron:
http://www.stibbeblog.nl/all-blog-posts/environment-and-planning/faq-wanneer-moet-een-ongewoon-voorval-op-grond-van-de-wet-milieubeheer-gemeld-worden/

Wanneer moet een ongewoon voorval op grond van de Wet milieubeheer (Wm) gemeld worden?
Een incident zit in een klein hoekje. Een ogenschijnlijk klein incident in een inrichting kan echter grote gevolgen met zich brengen. Als zich binnen een inrichting een ongewoon voorval voordoet, is de drijver van die inrichting verplicht om dat ongewone voorval aan het bevoegd gezag te melden. In de praktijk levert dit met enige regelmaat vragen op, want wanneer is een voorval zo ongewoon dat het gemeld moet worden? In dit blogbericht zetten wij uiteen wat deze verplichting in de praktijk betekent en hoe de meldplicht ingeperkt kan worden. Daarnaast geven we een checklist waarmee een bedrijf kan nalopen of zij een ongewoon voorval moet melden.
De meldplicht van artikel 17.2 Wm houdt in dat ongewone voorvallen zo spoedig mogelijk bij het bevoegd gezag moeten worden gemeld. Het gaat om die ongewone voorvallen die zich binnen een inrichting hebben voorgedaan én die nadelige gevolgen voor het milieu hebben of kunnen hebben. Uit de wet volgt dus niet wanneer en binnen welke termijn moet worden gemeld. Dit wordt bepaald door de invulling van open normen en deze invulling kan aanleiding geven tot discussie. Hoe deze normen in de praktijk door het bevoegd gezag worden ingevuld, volgt hieronder.

Wat is een ongewoon voorval?
Wanneer sprake is van een ongewoon voorval is in de wet niet gedefinieerd. Wat dan wel onder ongewoon voorval moet worden verstaan, heeft de Afdeling bestuursrechtspraak van de Raad van State (hierna: de Afdeling) in haar vaste jurisprudentie bepaald. Volgens de Afdeling is een ongewoon voorval ‘elke gebeurtenis in een inrichting, ongeacht de oorzaak daarvan, die afwijkt van de normale bedrijfsactiviteiten; dit begrip omvat derhalve zowel storingen in het productieproces en storingen in de voorzieningen van de inrichting als ongelukken en calamiteiten.’
Er is dus al gauw sprake van een ongewoon voorval, want zodra een voorval afwijkt van de normale bedrijfsactiviteiten is het al ongewoon. Een onschuldig incident, zoals het morsen van een bepaalde stof, kan hier ook onder vallen.

Wanneer is sprake van nadelige gevolgen voor het milieu?
Een ongewoon voorval hoeft alleen gemeld te worden als het ongewone voorval nadelige gevolgen voor het milieu heeft of kan hebben.
Wanneer sprake is van gevolgen voor het milieu is gedefinieerd in artikel 1.1 lid 2 sub a en sub b Wm. Hiermee worden álle mogelijke gevolgen voor het milieu bedoeld (Kamerstukken II 1988,89, 21 087, nr. 3, p. 31). Hiervan kan gauw sprake zijn.
Indien is vastgesteld dat er sprake is van gevolgen voor het milieu, is de volgende stap dat vastgesteld moet worden of deze gevolgen ook nadelig zijn. Dit is afhankelijk van de omstandigheden en verschilt per ongewoon voorval. Uit jurisprudentie van de Afdeling volgt in ieder geval dat niet ieder gevolg voor het milieu nadelig hoeft te zijn. Bijvoorbeeld als door de geringe hoeveelheid gelekte stof en de opvang en afvoer daarvan geen nadelige gevolgen voor het milieu zijn ontstaan.

Gevolgen buiten de inrichting?
Goed om te realiseren is dat het begrip 'milieu' volgens vaste jurisprudentie van de Afdeling, zijn begrenzing vindt in het begrip 'inrichting'. Dat betekent dat de meldingsplicht alleen ziet op nadelige gevolgen voor het milieu buiten de inrichting.

Causaal verband?
Tot slot moeten de nadelige gevolgen toe te rekenen zijn aan het ongewone voorval. Met andere woorden, er moet sprake zijn van een causaal verband tussen het ongewone voorval en de nadelige gevolgen voor het milieu.

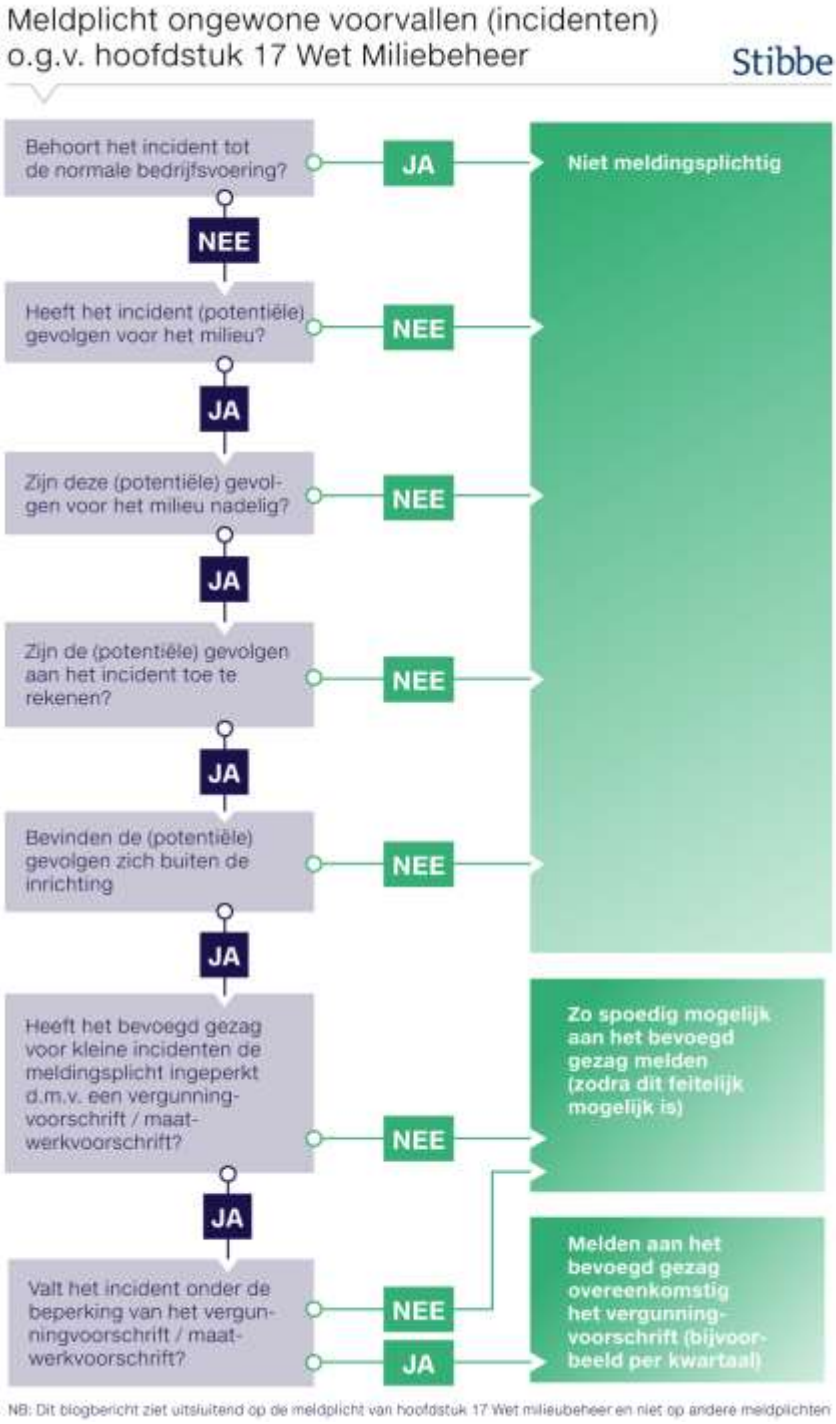
Hoe 'spoedig' moet het ongewone voorval gemeld worden?
De drijver van een inrichting moet het ongewone voorval zo spoedig mogelijk aan het bevoegd gezag melden. Wanneer hieraan is voldaan, volgt niet uit de wettelijke bepaling. Uit jurisprudentie is af te leiden dat zo spoedig mogelijk betekent zodra dit mogelijk is. Wanneer dit mogelijk is, hangt af van de omstandigheden van het geval. In de literatuur wordt de opvatting gehuldigd dat dit betekent, zodra dit feitelijk mogelijk is (AB 2005/80, m.nt. F.C.M.A. Michiels). In de praktijk wil dit nog wel eens misgaan, omdat een bedrijf zich niet of te laat realiseert dat een voorval meldingsplichtig is. Overtreding van de meldplicht kan zowel bestuursrechtelijk als strafrechtelijk worden gehandhaafd; het is dus zaak hier alert op te zijn!

Reikwijdte van de meldplicht?
In een inrichting komen ook kleine incidenten voor. De nadelige gevolgen voor het milieu van deze kleine incidenten zijn niet altijd significant. Toch zijn deze kleine incidenten op grond van artikel 17.2 Wm wel meldingsplichtig.
Het werd door zowel de praktijk als de wetgever als onnodig belastend ervaren dat al deze ongewone voorvallen zonder merkbare milieueffecten, onmiddellijk gemeld moesten worden. Daarom is in 2011 de mogelijkheid in de wet opgenomen om de ruime meldplicht in te perken (artikel 17.2 lid 4 Wm, ingevoegd bij Kamerstukken II 2009-2010, 32 445, nr. 3, p. 3).
Op grond van dit artikel kan het bevoegd gezag voor deze kleine incidenten een afwijkende regeling treffen. Deze afwijkende regeling houdt in dat deze kleine incidenten pas binnen een bepaalde termijn moeten worden gemeld of geregistreerd. Het bevoegd gezag kan bijvoorbeeld een vergunningvoorschrift aan de omgevingsvergunning verbinden of een maatwerkvoorschrift stellen. Deze beperking van de meldplicht kan een enorm voordeel voor een inrichting betekenen. Zoals gezegd, is overtreding van de meldplicht zowel bestuursrechtelijk als strafrechtelijk handhaafbaar. Daarom is het zonde dat in de praktijk nog maar beperkt gebruik wordt gemaakt van de mogelijkheid tot inperking van de meldplicht om handhaving te voorkomen. Daarom adviseren wij drijvers van inrichtingen in overleg te treden met het bevoegd gezag om te kijken welke mogelijke beperkingen op de meldplicht kunnen worden gemaakt.

Blik op de toekomst: de Omgevingswet
Afdeling 19.1 van de nieuwe Omgevingswet ziet op ongewone voorvallen. Het begrip 'ongewoon voorval' wordt in de bijlage bij de Omgevingswet gedefinieerd als een gebeurtenis, ongeacht de oorzaak daarvan, die afwijkt van het normale verloop van een activiteit, zoals een storing, ongeluk of calamiteit waardoor significante nadelige gevolgen voor de fysieke leefomgeving ontstaan of dreigen te ontstaan. Specifiek worden genoemd een inbreuk op de vergunningsvoorwaarden (als bedoeld in artikel 8 van de Richtlijn Industriële Emissies) of een zwaar ongeval (als bedoeld in artikel 3, onderdeel 13, van de Seveso-richtlijn). Met deze definitie wordt het begrip 'ongewoon voorval' breder dan nu het geval is.

Op grond van artikel 2.16 van het Ontwerpbesluit activiteiten leefomgeving moeten ongewone voorvallen gemeld worden. Het artikel luidt als volgt:
"Artikel 2.16 (informeren over een ongewoon voorval)
Het bevoegd gezag of de commissaris van de Koning, voor zover het ongewoon voorval betrekking heeft op luchtverontreiniging, wordt onverwijld geïnformeerd over een ongewoon voorval."
Uit de artikelsgewijze Nota van Toelichting bij het Ontwerpbesluit activiteiten leefomgeving blijkt dat met voornoemde meldingsplicht geen wijziging is beoogd ten opzichte van de regeling, zoals die nu geldt op grond van artikel 17.2 Wet milieubeheer. In een afzonderlijk blogbericht wordt nader ingegaan deze meldplicht.

Checklist: moet een incident gemeld worden?
Aan de hand van onderstaande visual kan gecheckt worden of een incident gemeld moet worden.



NB: Dit blogbericht ziet uitsluitend op de meldplicht van hoofdstuk 17 Wet milieubeheer en niet op andere meldplichten

129. Milieu. Activiteiten Internet Module (AIM)

Wat zegt de AP over AIM?
Geen specifieke informatie

Wat zeggen andere belanghebbenden over AIM en AVG?

- https://www.infomil.nl/onderwerpen/integrale/omgevingsloket/vragen-antwoorden/bedrijven/algemene-verordening/betekent-avg-bevoegd/
- https://www.infomil.nl/onderwerpen/integrale/omgevingsloket/vragen-antwoorden/bedrijven/algemene-verordening/

Moeten gemeenten en andere bevoegd gezagen die gebruik maken van het OLO en AIM, hiervoor een 'verwerkersovereenkomst' met het ministerie opstellen?
In Omgevingsloket online (OLO) en de activiteiten internet module (AIM) kan een burger of bedrijf digitaal een aanvraag of melding doen voor omgevingsvergunningen en watervergunningen. De verdere afhandeling van de aanvraag of melding vindt plaats bij het bevoegd gezag dat de toestemming of vergunning verleent. Omgevingsloket online en de AIM zijn de 'postbus' die de gegevens doorgeleiden naar het bevoegd gezag. De betrokken ministeries (BZK voor OLO en I&W voor de AIM) hebben als verwerkersverantwoordelijke een registratie opgesteld voor de werking van de loketten. Het bevoegd gezag is na ontvangst van de aanvragen/meldingen zelf verantwoordelijk voor het conform de AVG omgaan met de gegevens.

Mag een bedrijf, als gemachtigde, vragen om het BSN?
Dat mag. Om een aanvraag te doen voor een particulier of namens een particulier wordt in het aanvraagformulier gevraagd het burgerservicenummer (BSN) van de particuliere aanvrager in te vullen. Dit is een vereiste uit de regelgeving en kan niet worden overgeslagen.

Omgevingsloket online en de Algemene verordening gegevensbescherming (AVG)
Omgevingsloket online vraagt om de persoonsgegevens op grond van de regels in de Algemene wet bestuursrecht, de Wet algemene bepalingen omgevingsrecht en de Waterwet.

Waar is bepaald dat persoonsgegevens moeten worden opgenomen in de publiceerbare aanvraag/ melding?
In de wetgeving is bepaald dat een aanvraag bepaalde persoonsgegevens moet bevatten om de aanvraag in behandeling te kunnen nemen.

Is het mogelijk een toestemming voor de publicatie van persoonsgegevens in te trekken?
Dit is niet mogelijk. In het geval u zich bedenkt en gegevens niet openbaar gemaakt wil hebben bij publicatie, neem dan contact op met het bevoegd gezag.

130. Voedselveiligheid

Wat zegt de AP over Voedselveiligheid?
Geen specifieke informatie

Bron:
https://www.kleemans.nl/nieuws/avg-en-bezoekregistratie/
https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers_nl

Valt bezoekersregistratie als onderdeel van certificeringssystemen op basis van BRC of IFS bij leveranciers onder de AVG?
Dat is afhankelijk van wat er naderhand met de lijsten wordt gedaan; worden deze handmatig bewaard zonder classificatie of digitaal geregistreerd dan valt dit niet onder de AVG zolang de gegevens verder niet verwerkt worden. Als het bezoekregister wel wordt geclassificeerd en verwerkt (denk aan bezoekersanalyse e.d.) dan is de kans groot dat dit wel onder de AVG valt.

131. Onderzoek mogelijke fraude werknemer

Wat zegt de AP over Voedselveiligheid?
Geen specifieke informatie

Bron:
https://www.lenaadvocaten.nl/wp-content/uploads/2014/07/dilemmasdetectives.pdf

Jurisprudentie:

- EHRM 16 december 1992, NJ 1993, 400 (Niemietz), EHRM 25 juni 1997, NJ 1998, 506 (Halford) en EHRM 3 april 2007, JAR 2007,233 (Copland); F.M.Teeuwen, 'Onrechtmatig verkregen bewijs in het arbeidsrecht', Arbeid Integraal 2008, p. 5-24;
- Conservatoir beslag door werkgever op woning werknemers onrechtmatig, wettelijke grondslag huiszoeking ondeugdelijk en onderzoek Hofmann Bedrijfsrecherche in strijd met art. 10 Gw, Hof
  Leeuwarden 4 augustus 2009, LJN: BJ4901.

Wat moet voor de start van een onderzoek naar een werknemer worden beoordeeld?
Te beoordelen of wordt voldaan aan de juridische normen in de volgende drie categorieën:

1. Normen die het onderzoek motiveren en legitimeren ('toetsingsnormen').
    a. Grondslag voor onderzoek naar gedragingen van de werknemer is dat een werkgever op grond van de bevoegdheid om ordevoorschriften te geven (art. 7:660 BW) in het verlengde daarvan de bevoegdheid heeft om te controleren of deze regels worden nageleefd
    b. Bepalingen over ziekte en re-integratie (art. 7:628, 7:629 en 7:658a BW). Deze bepalingen impliceren enerzijds een verplichting om loon door te betalen bij ziekte en anderzijds een bevoegdheid om dit niet te doen als de werknemer niet ziek is of onvoldoende meewerkt aan zijn re-integratie. Aangezien de werkgever moet kunnen vaststellen of de werknemer daadwerkelijk recht heeft op loondoorbetaling, ligt het voor de hand te veronderstellen dat hij ook vanwege deze regels bevoegd is om het vermoeden van niet-ziekte te onderzoeken.
2. Normen die het onderzoek begrenzen ('grensnormen'):
    1. art. 10 Grondwet
    2. art. 8 EVRM
    3. Jurisprudentie Europese Hof voor de rechten van de mens (EHRM)
    4. AVG
    5. Jurisprudentie AVG
3. Normen die bepalen of, en zo ja, welk gewicht het onderzoek in een civiele procedure heeft ('procedurele normen')
    1. stel de concrete aanleiding voorhet onderzoek vast;
    2. onderzoek of er (interne) richtlijnen, cao-bepalingen of procedures voor een onderzoek bestaan;
    3. ga na of het onderzoek een legitiem doel dient;
    4. ga na of het belang van de werkgever bij het te bereiken doel opweegt tegen de te plegen inbreuk op de privacy van de werknemer (proportionaliteitsbeginsel);
    5. ga na of het doel op een minder ingrijpende wijze kan worden bereikt (subsidiariteitsbeginsel);
    6. controleer of het (externe) onderzoeksbureau conform een gedragscode dan wel gedragsrichtlijn handelt;

7. wees kritisch ten aanzien van de formulering van de onderzoeksopdracht en beperk de reikwijdte zodanig dat onnodige privacyschending wordt voorkomen;
8. maak heldere afspraken over tijdschema, kosten, naleving AVG en de te gebruiken onderzoeksmiddelen, waarbij proportionaliteits- en subsidiariteitsbeginsel leidend zijn;
9. zorg ervoor dat de rapportage zich beperkt tot vastlegging van die feitelijke waarnemingen die relevant zijn voor de opdrachtgever, zonder waardeoordeel;
10. houd duur en omvang van het onderzoek voortdurend in de gaten en handel voortvarend;
11. laat niet meer technische hulpmiddelen inzetten dan nodig en probeer inbreuk op de persoonlijke intieme levenssfeer zo veel mogelijk te vermijden;
12. informeer de werknemer indien en zodra het onderzoek dat toelaat, over het onderzoek en het feit dat persoonsgegevens zijn verwerkt;
13. stel de werknemer altijd in staat om te worden gehoord en zich van juridische bijstand te voorzien;
14. betrek de visie van de werknemer in de rapportage (hoorplicht);
15. stel de werknemer in de gelegenheid om documenten uit het bedrijf van de werkgever op te vragen en deze te bestuderen, tenzij een zwaarwichtig (onderzoeks)belang
zich daartegen verzet;
16. verstrek een afschrift van de onderzoeksrapportage aan de werknemer;
17. formuleer conclusies nadat de werknemer is gehoord en handel (wederom) voortvarend.

Hoever strekt het grondrecht privacy zich uit volgend het Europese Hof voor de rechten van de mens (EHRM)?
Het voornaamste individuele recht van de werknemer dat tijdens een onderzoek in het gedrang zal komen, is het recht op privacy. Tijdens het onderzoek zal het onderzoeksbureau onder meer in aanraking komen met het grondrecht van privacy (art. 10 Grondwet en art. 8 EVRM), inhoudende dat een ieder recht heeft op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en correspondentie. Het Europese Hof voor de rechten van de mens (EHRM) heeft beslist dat het recht op privacy van een werknemer zich ook uitstrekt tot de werkplek en zakelijke correspondentie. In onder meer de zaken Halford en Copland heeft het EHRM uitgemaakt dat werknemers een redelijke verwachting van bescherming van die privacy mogen hebben.

Wanneer is controle van werknemers toegestaan?
Voordat je als werkgever besluit te starten met de controle moet je het doel bepalen waarvoor de controle noodzakelijk is. De doelen moeten zijn bepaald voordat gegevens worden verwerkt. Het doel bepaalt de omvang van de controle en op welke wijze dat mag gebeuren. Let er daarbij op dat de doelen niet te beperkt worden bepaald en dat die in het verwerkingsregister worden vermeld. Bijvoorbeeld: bescherming van bedrijfseigendommen, netwerkbeveiliging, opsporing en bestrijding van diefstal of verduistering, etc. Je dient altijd vooraf te onderzoeken of het controlemiddel dat je wil instellen noodzakelijk is. Ofwel, er mag geen andere manier zijn (dat minder vergaand en minder ingrijpend is) om het doel te bereiken. Als blijkt dat er wel een andere, minder ingrijpende, wijze is om het doel te behalen, dan mag je niet overgaan tot het inzetten van het controlemiddel.

Ook moet je een gerechtvaardigd belang hebben voor het inzetten van het controlemiddel. Vooraf dien je te onderzoeken of dit belang zwaarder weegt dan het privacybelang van de werknemer(s). Deze belangenafweging moet je ook vastleggen.

Een andere voorwaarde voor de inzet van een controlemiddel is dat de voorafgaande instemming van de ondernemingsraad (OR) moet zijn gevraagd.
Daarnaast zal je het personeel moeten informeren over wat is toegestaan en wat is verboden, dat controle mogelijk is en op welke manier dat gebeurt. Dit kan bijvoorbeeld met gedragsregels of in een protocol.

Wat zijn de verplichtingen zodra je besluit om grootschalige en/of systematische controle uit te voeren, bijvoorbeeld om diefstal en/of fraude binnen het bedrijf te voorkomen?
Dan ben je als werkgever verplicht om vooraf een zogenaamde DPIA (Data Protection Impact Assessment, ook PIA genoemd) uit te voeren. Dat is een risicobeoordeling van de privacy-effecten van deze controle voor de werknemers. Ik verwijs daarvoor ook naar onze eerdere blogpost. Als uit de DPIA moet worden geconcludeerd dat de beoogde controle een hoog risico oplevert en je geen maatregelen kan nemen die dat risico beperken, dan moet je de Autoriteit Persoonsgegevens (AP) voorafgaand raadplegen. Ook moet de bewaartermijn in acht worden genomen. Regel is dat de persoonsgegevens niet langer dan noodzakelijk mogen worden bewaard. Voor camerabeelden geldt als regel maximaal vier weken. Tenzij een incident op de beelden is vastgelegd, dan mag je de beelden bewaren tot het incident is afgehandeld.

132. Vergunning door AP

Wat zegt de AP over vergunning door AP?

- https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/vergunning-aanvragen
- https://autoriteitpersoonsgegevens.nl/nl/publicaties/register-vergunningen
- https://autoriteitpersoonsgegevens.nl/nl/nieuws/vergunning-voor-financiele-instellingen-om-info-over-fraude-te-delen
- https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/zwarte-lijst
- https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handreiking_cross-sectorale_zwarte_lijsten.pdf

Bron:

- https://meld.nl/hoe-werkt-het/
- https://www.rijksoverheid.nl/contact/contactgids/fraudehelpdesk
- https://www.rvig.nl/fraudebestrijding/centraal-meldpunt-identiteitsfraude-en--fouten
- https://www.fiod.nl/ik-wil-fraude-melden/
- https://www.fraudehelpdesk.nl/

Waarom heeft de Fraudehelpdesk de dienstverlening sinds 29 juli 2019 aangepast?
In verband met de verscherpte Europese privacywetgeving past de Fraudehelpdesk per direct een deel van zijn werkzaamheden aan met betrekking tot het vastleggen van fraudemeldingen en het publiceren van waarschuwingen.
In de Algemene verordening gegevensbescherming (AVG) gelden namelijk bijzondere richtlijnen voor het vastleggen van strafrechtelijke persoonsgegevens. Omdat wij deze gegevens ontvangen in meldingen van burgers en ondernemers raakt de AVG de dienstverlening van de Fraudehelpdesk.
Om deze gegevens te mogen registreren en verwerken hebben we bij de Autoriteit Persoonsgegevens een vergunning aangevraagd. Deze vergunning is ons niet verleend en daarom hebben we onze werkprocessen en werkwijzen inmiddels aangepast volgens de geldende wetgeving.
We leggen vanaf nu geen informatie meer vast over mogelijk frauderende partijen en delen deze informatie niet meer met de politie als die daarom verzoekt. Daarnaast publiceren wij geen spooknota's en nep-facturen meer op onze website. Het betekent ook dat we zijn gestopt met het geautomatiseerd ontvangen en publiceren van valse e-mails (phishingmails). Dat de Fraudehelpdesk deze dienst niet meer uitvoert, is direct merkbaar voor vele burgers en bedrijven in Nederland. We ontvingen namelijk maandelijks gemiddeld ruim 80.000 e-mails waarvan de echtheid geautomatiseerd geverifieerd werd en waarvoor we waarschuwden via onze website en social media.
We respecteren het besluit van de Autoriteit Persoonsgegevens maar zijn ook teleurgesteld dat het belang van de fraudeur zwaarder lijkt te wegen dan dat van het slachtoffer. Toch roepen we burgers op om fraude vooral te blijven melden bij de Fraudehelpdesk. Onze medewerkers blijven melders binnen de mogelijkheden van de wet zo adequaat mogelijk helpen.
Om ons werk nog beter te kunnen uitvoeren, zouden wij meldingen die binnenkomen wel graag volledig willen vastleggen, de informatie willen verwerken en het systeem om phishing vast te stellen en ervoor te waarschuwen weer in gebruik willen nemen.
De Fraudehelpdesk gaat voor de verschillende werkzaamheden opnieuw een vergunning aanvragen bij de Autoriteit Persoonsgegevens.
Ons is er alles aan gelegen om onze dienstverlening optimaal uit te voeren: fraude beter en sneller signaleren en in een eerder stadium helpen voorkomen. Naast het adviseren en doorverwijzen van melders is fraudepreventie namelijk onze belangrijkste taak.

133. Standaard contract clausules

Wat zegt de AP over vergunning door SCC?

- https://autoriteitpersoonsgegevens.nl/nl/nieuws/nieuw-modelcontract-voor-veilige-doorgifte-persoonsgegevens
- https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/infographic_data_transfers.pdf

Bron:

- https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries
- https://ploum.nl/kenniscentrum/nieuws/europese-commissie-neemt-nieuwe-modelbepalingen-standard-contractual-clauses-voor-gegevensdoorgiften-naar-derde-landen-aan?utm_medium=email

Waarom nieuwe Standard Contractual Clauses (SCC's) in 2021?
De Europese Commissie heeft op 4 juni 2021 nieuwe Standard Contractual Clauses (hierna afgekort tot SCC's) aangenomen. Om het belang van deze nieuwe SCC's goed te begrijpen is het goed om kort stil te staan bij de functie van de SCC's in het algemeen.
De SCC's vormen een modelcontract dat kan worden gebruikt om de waarborgen te bieden die hoofdstuk 5 van de Algemene Verordening Gegevensbescherming (AVG) vereist voor het doorgeven van gegevens vanuit de EER naar landen buiten de Europese Economische Ruimte (EER). Persoonsgegevens mogen onder de AVG niet zomaar naar landen buiten de EER (ook wel: derde landen) worden doorgegeven. Gegevens mogen enkel worden doorgegeven wanneer gewaarborgd is dat de gegevens ook in het derde land voldoende beschermd worden. Dit is bijvoorbeeld het geval wanneer de Europese Commissie een adequaatheidsbesluit uitvaardigt ten behoeve van dat derde land. Wanneer er geen adequaatheidsbesluit bestaat ten aanzien van het derde land waaraan de gegevens worden doorgegeven, kunnen (onder meer) middels de SCC's afspraken worden gemaakt met de partij die de persoonsgegevens ontvangt. Dat kan een andere 'verwerkingsverantwoordelijke' of een 'verwerker' (zoals bijvoorbeeld een softwareleverancier) zijn. Deze afspraken moeten ervoor zorgen dat de vertrouwelijkheid, integriteit en beschikbaarheid van die gegevens voldoende wordt beschermd.
De oude SCC's, die al een behoorlijke tijd meegingen, waren aan vervanging toe. In de Schrems II uitspraak van het Europese Hof van Justitie kwam ook naar voren dat niet alleen goede afspraken moeten worden gemaakt tussen de gegevensexporteur en -importeur, maar ook dat beoordeeld moet worden of deze afspraken de gewenste uitwerking zullen hebben in het licht van de wetgeving in het land waar de gegevens naartoe worden gestuurd. Veelal zijn dan nog aanvullende maatregelen vereist, wat in de nieuwe SCC's duidelijker naar voren is gebracht. Hierover heeft de EDPB inmiddels ook richtlijnen gepubliceerd.

Wat is er veranderd ten opzichte van de oude SCC's?
De nieuwe SCC's omvatten een aantal nieuwe bepalingen die met name zijn toegevoegd naar aanleiding van de Schrems II uitspraak. Maar niet alleen qua inhoud zijn er wijzigingen doorgevoerd, ook de vorm van de SCC's is gewijzigd.
Anders dan voorheen is er nu één set SCC's met daarin de bepalingen voor alle varianten van doorgiften (verwerkingsverantwoordelijke-verwerker, verwerkingsverantwoordelijke-verwerkingsverantwoordelijke, verwerker-verwerkingsverantwoordelijke en verwerker-verwerker),

waar er voorheen voor verschillende varianten een eigen set SCC's bestond – en voor bijvoorbeeld de relatie verwerker-subverwerker geen officieel modelcontract bestond.
Bij de nieuwe SCC's moeten partijen dus onderling afspreken welke specifieke bepalingen van toepassing zijn.
Er zijn ook nieuwe bepalingen in dit modelcontract opgenomen. Zo is een bepaling opgenomen die verplicht tot het doen van een Data Transfer Impact Assessment (DTIA). Daarnaast zijn er bepalingen toegevoegd die zien op de toegang tot persoonsgegevens door autoriteiten. Zo moeten gegevensimporteurs zowel de exporteur als betrokkenen informeren ingeval van een verzoek tot inzage door de autoriteiten, moet de importeur de legaliteit van het inzageverzoek onderzoeken (en verplicht ageren tegen dat verzoek indien daartoe grond bestaat) en ingeval aan een verzoek gehoor dient te worden gegeven dienen enkel de minimale verplichte gegevens te worden getoond.
Hiermee hebben zijn een aantal bepalingen uitgelicht, maar niet alle veranderingen besproken. Het is goed om de relevante bepalingen voor een specifieke verwerkingsrelatie door te nemen.

Wat als bedrijf nu het beste kan doen naar aanleiding van het aannemen van deze SCC's?
De nieuwe SCC's zijn nu dus aangenomen en gepubliceerd door de Europese Commissie. Deze kunnen nu worden gebruikt. Tot 27 september 2021 geldt een overgangsperiode en kunnen ook de oude SCC's nog worden gesloten. Vanaf 27 september 2021 hebben partijen die de oude SCC's gebruiken 15 maanden de tijd om deze nieuwe SCC's te sluiten die de oude vervangen. Let wel, hierbij geldt dat de verwerkingsactiviteiten niet mogen veranderen en (ook bij gebruik van de oude SCC's) is het nodig dat dit gebruik van SCC's toereikende waarborgen ter bescherming van de privacy van betrokkenen biedt.
Omdat in HvJ Schrems II bepaald is dat die oude SCC's onvoldoende waarborgen bieden, is het wel raadzaam om zo snel mogelijk over te stappen en nieuwe afspraken te maken als data importeur of exporteur.

Wat is het adequaatheidsbesluit?
Persoonsgegevens worden niet overal in de wereld beschermd op een niveau dat wij in de EU gewend zijn. Binnen de EU geldt één set aan regels, namelijk de AVG. Daarom is het geen probleem om persoonsgegevens te (laten) verwerken in bijvoorbeeld Finland of op Cyprus. Voor doorgifte naar een land buiten de EU gelden andere regels. Derde landen zijn alle landen buiten de EU met uitzondering van de landen in de Europese Economische Ruimte (EER): IJsland, Liechtenstein en Noorwegen. Doorgifte van persoonsgegevens vanuit Nederland naar een derde land mag in principe alleen als het derde land een passend beschermingsniveau biedt. De Europese Commissie kan een adequaatheidsbesluit nemen als een derde land in de nationale wetgeving een passend niveau van gegevensbescherming biedt. Dat houdt in dat de Europese Commissie vaststelt dat het land een vergelijkbaar gegevensbeschermingsniveau biedt als de AVG. De landenlijst met een passend beschermingsniveau vindt je op https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#dataprotectionincountriesoutsidetheeu

Wat zijn Standard Contractual Clauses (SCC)
De SCC zijn in feite modelcontracten die goedgekeurd zijn door de Europese Commissie. Zij bieden de aanvullende, contractuele waarborgen voor gegevensbescherming als persoonsgegevens vanuit de EER naar een derde land worden doorgegeven. SCC kunnen echter niet zomaar worden gebruikt. Sinds de ongeldigverklaring van het Privacy Shield is een beoordeling nodig van de privacy risico's die kunnen ontstaan wanneer overheidsinstanties van het land waarnaar de gegevens worden doorgegeven, toegang krijgen tot persoonsgegevens, en hoe zulke risico's kunnen worden gemitigeerd. Naar aanleiding van het resultaat op het risico-assessment kunnen aanvullende technische en organisatorische maatregelen noodzakelijk zijn. Om de privacy risico's te

ondervangen, kan mogelijk gebruik worden gemaakt van contractuele, technische en organisatorische aanvullende maatregelen zoals certificeringen, encrypties of garanties, waarin de geschiktheid van de maatregelen die de gegevens importerende partij heeft genomen zijn beoordeeld. Als deze maatregelen niet haalbaar blijken in het licht van het verminderen van risico's, mag de doorgifte van persoonsgegevens niet plaatsvinden. De European Data Protection Board heeft:

- Aanbevelingen opgesteld https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en
- Richtlijn opgesteld waarin is opgenomen hoe de risico's van derde landen dienen te worden geïdentificeerd en beoordeeld: en https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-102020-restrictions-under-article-23-gdpr_en

134. Begrippenlijst

Bron:

- https://www.beterbenutten.nl/assets/upload/IMMA-Leidraad-omgaan-met-persoonsgegvens-2018.pdf
- https://www.fgsupport.nl/begrippenlijst
- https://www.nldigital.nl/news/begrippenlijst-avg/

Begrip	Toelichting
Accountability	(Documentatieplicht) bedrijven moeten zelf kunnen laten zien dat ze voldoen aan de privacywetgeving. Je kunt daarbij gebruikmaken van het Voorbeeldregister verwerkingen voor de verwerker.
Anonimiseren	Dit is een speciale verwerking van persoonsgegevens. Wat je doet met anonimiseren, is een persoonsgegeven zó veranderen, dat je niet meer kunt achterhalen over wie het betreffende gegeven gaat. Als gegevens eenmaal geanonimiseerd zijn, zijn het geen persoonsgegevens meer, en is de AVG niet meer van toepassing.
AP	Autoriteit Persoonsgegevens, de Nederlandse toezichthouder op de naleving van de Algemene Verordening Gegevensbescherming. Sinds de inwerkingtreding van de Algemene Verordening Gegevensbescherming heeft de AP een uitgebreidere boetebevoegdheid.
AVG	Algemene Verordening Gegevensbescherming. De Europese privacy verordening die sinds 25 mei 2018 de Wet bescherming persoonsgegevens vervangt. Deze verordening is direct toepasbaar in de nationale rechtsorde van EU-lidstaten, maar laat op bepaalde gebieden ruimte voor implementatieverschillen. Voor Nederland zijn deze verschillen opgenomen in de Uitvoeringswet AVG.
Betrokkene / datasubject	De persoon op wie de gegevens betrekking hebben. Dit kan een consument zijn maar ook een medewerker van een bedrijf (bijvoorbeeld een medewerker wiens verplaatsingen worden gevolgd ten behoeve van fleetmanagement).
Bijzondere persoonsgegevens	De AVG refereert aan gevoelige persoonsgegevens als “speciale categorieën van persoonsgegevens.” De speciale categorieën van persoonsgegevens omvatten ras of etnische afkomst, politieke opvattingen, religie of levensbeschouwelijk opvattingen, lidmaatschap van een vakbond, seksuele gerichtheid, en gezondheid, genetische en biometrische gegevens waar verwerkt tot een uniek te identificeren individu. Persoonsgegevens gerelateerd tot criminele veroordelingen en overtredingen zijn niet inbegrepen, maar verglijkbare waarborgen zijn hier van toepassing.
Biometrische gegevens	Persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedrag gerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens.

Begrip	Toelichting
Cookie	Kleine tekstbestanden die op de computer, mobiele telefoon, tablet of ander apparaat van een gebruiker kunnen worden geplaatst met als doel het identificeren van het apparaat.
Cookiewet	De regels over cookies zijn opgenomen in art. 11.7a van de Telecommunicatiewet, kortweg ook vaak de Cookiewet genoemd. In deze wet wordt het gebruik van cookies gereguleerd. Deze wetgeving wordt de komende jaren vervangen door de Europese ePrivacy Verordening, die naar verwachting vanaf 2020 gaat gelden.
DPIA	DPIA staat voor data protection impact assessment. In de AVG wordt dit de gegevensbeschermingseffectbeoordeling genoemd. Deze beoordeling is verplicht wanneer sprake is van een verwerking van persoonsgegevens met een hoog risico voor de rechten en vrijheden van betrokkenen, bijvoorbeeld bij stelselmatige en grootschalige monitoring van openbare ruimten.
Derde	Degene die niet de betrokkene, de verwerkingsverantwoordelijke of de verwerker is. Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.
EDPB	De Europese Raad voor gegevensbescherming vervangt de Artikel 29 werkgroep, en hun functie zal inhouden om de consistentie te waarborgen in de toepassing van de AVG, het adviseren van de Europese Commissie, accrediteren van toezichthoudende instanties, en opinies geven ten aanzien van concept besluiten van toezichthoudende autoriteiten.
Genetische gegevens	Persoonsgegevens die verband houden met de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon.
Gezondheids-gegevens	Persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.
Inbreuk in verband met persoons-gegevens	Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens
Ontvanger	De derde aan wie persoonsgegevens worden doorgegeven.

Begrip	Toelichting
Persoonsgegevens	Alle informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Geïdentificeerd houdt in dat een natuurlijke persoon uniek te onderscheiden is van andere personen op basis van identificerende gegevens (bijvoorbeeld NAW). Identificeerbaar betekent dat een natuurlijke persoon direct of indirect kan worden geïdentificeerd ('to single out') door de verwerkingsverantwoordelijke en/of redelijkerwijs door derden, met name aan de hand van een identificator zoals een naam, identificatienummer, locatiegegevens, een online identificator of één of meer kenmerken van de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van deze persoon.
Profilering	Elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen
Pseudonimisering	Het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.
Recht op vergetelheid	Betrokkenen krijgen uitgebreidere rechten. Eén recht waar veel over gesproken wordt is *the right to be forgotton*. We hebben daarom een Handleiding Inzage- en verwijderverzoeken opgesteld.
Toestemming van de betrokkene	Elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt.
Verantwoording	Verantwoording (accountability) is het vermogen compliance aan te tonen met de AVG. De Verordening verklaart expliciet dat dit de verantwoordelijkheid is van de organisatie. Teneinde compliance aan te tonen, moeten afdoende technische en organisatorische maatregelen zijn geïmplementeerd. *Best practice*-instrumenten zoals de gegevensbeschermingseffectbeoordeling (DPIA of PIA) en ontwerp van gegevensbescherming zijn in bepaalde omstandigheden wettelijk vereist.

Begrip	Toelichting
Verwerker	Degene die ten behoeve van de verwerkingsverantwoordelijke Persoonsgegevens verwerkt. Dat wil zeggen: overeenkomstig de instructies van de verwerkingsverantwoordelijke en onder zijn (uitdrukkelijke) verantwoordelijkheid, zonder aan zijn rechtstreeks gezag te zijn onderworpen. *De verwerker is dus een buiten de organisatie van de verwerkingsverantwoordelijke staande persoon of instelling die geen hiërarchische relatie met de verwerkingsverantwoordelijke heeft, maar een opdrachtgever-opdrachtnemer relatie.* *Een medewerker van een organisatie die de verwerking zelf uitvoert wordt niet beschouwd als een verwerker in de zin van de AVG.*
Verwerkings-verantwoordelijke	De natuurlijke persoon, rechtspersoon of ieder ander die, of het bestuursorgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
Verwerking van persoonsgegevens	Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Hieronder valt het hele proces dat een persoonsgegeven doorloopt, vanaf het moment van verzamelen tot het moment van vernietigen. Al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

135. Bewaartermijnen

MAAS bewaart persoonsgegevens niet langer dan nodig. Hoe lang gegevens worden bewaard, is afhankelijk van wet- en regelgeving, de aard van de gegevens en de doeleinden waarvoor zij worden verwerkt. De bewaartermijn kan dus per doel verschillen. MAAS heeft een uitgebreid intern bewaarbeleid opgesteld. Wij hebben onze bewaartermijnen opgesteld aan de hand van uitgangspunten waaronder de looptijd van een contract, fiscale bewaartermijnen en het kunnen afhandelen van geschillen en klachten. E bewaartermijn zijn aangegeven in het MAAS AVG Verwerkingsregister.
Voor meer informatie over specifieke bewaartermijnen neem je contact op met de AVG.

Bewaartermijnen personeelsgegevens?
MAAS overzicht in het verwerkingsregister.

Bewaartermijnen medische gegevens?
MAAS overzicht in het verwerkingsregister.

Mag ik mijn medische gegevens laten vernietigen?
U kunt vragen om vernietiging van (een deel van) uw medisch dossier. Bijvoorbeeld als u niet wilt dat uw gegevens worden bewaard. Uw arts moet dit in de regel binnen 1 maand doen.

Mag arts verzoek om vernietiging weigeren?
Uw arts mag uw verzoek in uitzonderlijke gevallen weigeren, bijvoorbeeld als:

- de informatie in uw dossier erg belangrijk is voor een ander dan uzelf (bijvoorbeeld over erfelijke ziekten);
- er een wet is die een bewaartermijn voorschrijft, waarbinnen de gegevens niet vernietigd mogen worden. Bijvoorbeeld bij een gedwongen opname in een psychiatrisch ziekenhuis;
- de hulpverlener zich moet verdedigen in een procedure.

Bewaartermijnen financiële & fiscale gegevens?
MAAS overzicht in het verwerkingsregister.

Wat moet je met administratie doen na de bewaartermijnen?
De Belastingdienst moet gedurende zeven jaar de mogelijkheid hebben om gegevens in te kunnen zien. Na deze zeven jaar zal de Belastingdienst de basisgegevens niet meer opvragen. Als het bewaartermijn of de bewaarplicht van zeven jaar verstreken is kunt u de documenten (laten) vernietigen. Het advies is om uw administratie of boekhouding gecertificeerd te laten vernietigen door een professionele datavernietiger.

Bewaartermijn van vervoergegevens?
MAAS overzicht in het verwerkingsregister.

Bewaartermijnen logfiles computersystemen / e-mail en internetmonitoring?
MAAS overzicht in het verwerkingsregister.

Bewaartermijnen justitiële gegevens (gezien VOG, VGB)?
MAAS overzicht in het verwerkingsregister.

Bron:

https://www.justid.nl/onderwerpen/strafblad-en-het-justitieel-documentatie-systeem/hoelang-blijft-een-strafblad-bewaard

Wanneer worden justitiële gegevens van overtredingen verwijderd?

- 5 jaar na de einduitspraak of 5 jaar na het volledig betalen van een strafbeschikking;
- 10 jaar na de einduitspraak of 10 jaar na het volledig voldoen van een strafbeschikking als er een vrijheidsstraf of een taakstraf is opgelegd;
- 2 jaar na het overlijden van de persoon op wiens strafblad het feit staat.

Wanneer worden justitiële gegevens van misdrijven verwijderd?

De regels voor verwijdering van misdrijven zijn ingewikkelder dan bij overtredingen. De verwijderingstermijn hangt onder meer af van het strafmaximum dat voor dat feit in de wet staat. Dat is dus niet de straf die iemand kreeg maar de straf die iemand volgens de wet maximaal had kunnen krijgen.
Ook kan bij misdrijven de bewaartermijn verlengd worden als er een nieuwe einduitspraak wordt gedaan voor een ander misdrijf. De bewaartermijn van 20 en 30 jaar wordt namelijk verlengd als er een nieuwe einduitspraak volgt voor een ander strafbaar feit. Concreet betekent dit dat als er meerdere misdrijven staan geregistreerd, alle geregistreerde misdrijven pas worden verwijderd zodra de bewaartermijn, die het verst in de toekomst ligt, is verstreken. Dat heet verlenging of cumulatie.
Bij alle zedenmisdrijven (ongeacht de opgelegde straf of het strafmaximum), bij levenslange gevangenisstraf of wanneer een maatregel zoals TBS langer dan 40 jaar duurt: Na 80 jaar.

Bewaartermijnen pensioengegevens?

MAAS overzicht in het verwerkingsregister.

Welke gedragslijn volgen de pensioenfondsen?

Gedragslijn Verwerking Persoonsgegevens Pensioenfondsen Den Haag, 1 juli 2019. Deze Gedragslijn volgt op de eerder uitgebrachte servicedocumenten ‘Gegevensbescherming’ en ‘Guidance verwerking persoonsgegevens pensioenfondsen’. Deze Gedragslijn treedt in werking per 1 juli 2019. Pensioenfondsen hebben daarna 6 maanden de tijd om de Gedragslijn te implementeren. Per 1 januari 2020 rapporteren pensioenfondsen over de naleving van de Gedragslijn.

Kennen pensioenaanspraken geen wettelijke verjaringstermijnen?

Voor het vaststellen van toereikende bewaartermijnen moet rekening gehouden worden met zowel de belangen van de aanspraak- of pensioengerechtigde als met de belangen van het Pensioenfonds. Omdat pensioenaanspraken geen wettelijke verjaringstermijnen kennen, vraagt het vaststellen van de juiste termijnen om een lange termijn-benadering. Bijvoorbeeld in geval van pensionering, afkoop, echtscheiding en “vergeten pensioenen” is het van belang dat Pensioenfondsen c.q. uitvoerders kunnen reproduceren op welke wijze de pensioenopbouw heeft plaatsgevonden, waarop de berekeningen zijn gebaseerd, over welke deel van het salaris (incl. onkostenvergoedingen) pensioen is opgebouwd. Tussen het moment waarop zich een event (bijv. afkoop) voordoet en het moment dat er een geschil ontstaat, kan een periode van tientallen jaren liggen. Binnen deze termijn kunnen er vragen, aanspraken of geschillen ontstaan over de opgebouwde pensioenrechten.

Verwijzing in de wetgeving?

In artikel 59 Pensioenwet en in artikel 70 van de Wet verplichte beroepspensioenregeling is het volgende bepaald: ‘een rechtsvordering tegen een pensioenuitvoerder tot het doen van een uitkering verjaart niet bij leven van de pensioengerechtigde.’