Metaalunie-serie:

DE ALGEMENE VERORDENING GEGEVENSBESCHERMING

Algemeen deel en
Deel 2: Personeels- en loonadministratie

Hoewel de auteurs van deze uitgave uiterste zorg hebben betracht bij het samenstellen van dit document, aanvaardt Koninklijke Metaalunie geen aansprakelijkheid voor schade, van welke aard dan ook, die het directe of indirecte gevolg is van handelingen en/of beslissingen die (mede) gebaseerd zijn op de informatie in dit document.

In alle gevallen adviseren wij u, voordat u belangrijke zaken gaat aanpassen of regelen, vooraf contact op te nemen met de ledenadviseurs van Metaalunie.

Dit document is een uitgave van:

Koninklijke Metaalunie

Nederlandse organisatie van
ondernemers in het midden- en
kleinbedrijf in de metaal
Einsteinbaan 1
3439 NJ NIEUWEGEIN
Postbus 2600
3430 GA NIEUWEGEIN
Telefoon: (030) 605 33 44
Faxnummer: (030) 605 36 27
E-mailadres: bj@metaalunie.nl
Internetadres: www.metaalunie.nl

Inhoud

Inleiding

Vanaf 25 mei 2018 zal in Nederland de Algemene Verordening Gegevensbescherming van toepassing zijn. Deze verordening zal de Wet bescherming persoonsgegevens (Wbp) vervangen. De AVG regelt de privacy van personen in de gehele Europese Economische Ruimte[1] ("EER") op dezelfde manier.

De impact van de AVG op de gemiddelde mkb'er kan best groot zijn. Privacy lijkt voor veel ondernemers in de metaalbranche namelijk een onderbelicht onderwerp te zijn. Alle mkb'ers moeten nu ook al voldoen aan de Wbp, maar zijn daar in de praktijk vaak niet zo mee bezig.

De AVG is strenger dan de Wbp. De personen wiens gegevens worden verwerkt hebben meer rechten en de bedrijven die hun gegevens verwerken meer verantwoordelijkheden.

Om u te ondersteunen in de aanloop naar de AVG, zullen wij een serie uitbrengen waarin wij stapsgewijs aangeven hoe u zich op de komst van de AVG kunt voorbereiden. In ieder deel van de serie staat een ander administratief bedrijfsonderdeel centraal. Naast dat wij u voorzien van de benodigde basiskennis, zullen wij in chronologische volgorde de volgende administratieve processen behandelen (als daartoe aanleiding bestaat zullen wij van onderstaande indeling afwijken):

Algemeen deel	
Deel 1:	Klant- en leveranciersbeheer
Deel 2:	Personeels- en loonadministratie
Deel 3:	Overige verwerkingen/communicatie

In het algemene deel zullen wij u informeren over de begrippen die binnen de privacywetgeving een rol spelen, de belangrijkste aspecten van de AVG en een aantal algemene regels geven voor het omgaan met persoonsgegevens. Wij wijzen u er echter wel op dat dit algemene deel geen volledig overzicht geeft van alle regels en uitzonderingen die er binnen de AVG bestaan. Na het algemene deel volgen nog drie aparte delen in deze serie. In ieder deel zullen wij voor de hierboven genoemde administratieve onderdelen aangeven aan welke verplichtingen u moet voldoen en hoe. Daarbij nemen wij steeds een gemiddelde mkb'er als uitgangspunt. Wij noemen dit bedrijf metaalbedrijf Jansen. Wij hebben ervoor gekozen om een gemiddelde mkb'er centraal te stellen, omdat het beschrijven van alle mogelijke rechten en plichten voor alle denkbare situaties waarin onze achterban kan verkeren een dik boekwerk zal opleveren. Wij zullen daarom de kenmerken van metaalbedrijf Jansen schetsen, waarbij wij uiteraard zoveel mogelijk aansluiting zoeken bij de kenmerken van een gemiddeld Metaalunielid. Wij horen het natuurlijk graag als u van mening bent dat metaalbedrijf Jansen geen juiste weergave is van de gemiddelde mkb'er.

Voldoet u niet aan het geschetste profiel van metaalbedrijf Jansen, dan kunt u contact met ons opnemen om te bespreken op welke punt of welke punten u niet voldoet en wat dit betekent voor de aard en omvang van uw verplichtingen.

Ieder deel uit deze serie dat over een bepaalde verwerking gaat, is opgebouwd uit drie hoofdstukken: er zal eerst een omschrijving worden gegeven van het profiel van metaalbedrijf Jansen ten aanzien van het administratieve bedrijfsonderdeel dat aan de orde is. Voor uw gemak volgt daarna een "actiepuntenlijst". Zo kunt u meteen zien wat u te doen staat. Vervolgens kunt u een toelichting op de actiepunten nalezen in het laatste hoofdstuk van ieder deel.

Dan nog een laatste opmerking over de AVG. Doordat het om nieuwe wetgeving gaat, zijn er nog veel onduidelijkheden. De verwachting is dat de Autoriteit Persoonsgegevens ("AP"), de instantie die toezicht gaat houden op naleving van deze wet, in de aankomende periode een aantal van deze onduidelijkheden zal proberen weg te nemen. Ook de gezamenlijke Europese toezichthouders publiceren af en toe richtsnoeren ter verduidelijking van de nieuwe wet. Over andere onderwerpen zal mogelijk pas na gerechtelijke procedures duidelijkheid komen. In ieder geval zullen wij deze serie bij nieuwe ontwikkelingen aanpassen.

[1] EER: alle landen van de EU plus Liechtenstein, Noorwegen en IJsland.

ALGEMEEN DEEL

(De tekst van dit algemeen deel was ook onderdeel van de vorige checklist die over de klant- en leveranciersadministratie ging. Om het u bij het lezen van deze tweede checklist gemakkelijk te maken informatie terug te vinden uit het algemeen deel, hebben we de tekst uit dit deel opnieuw bijgevoegd)

Hoofdstuk 1: Begrippen, grondslagen en beginselen

§ 1.1. Algemeen

Als we het hebben over privacy dan draait het allemaal om "het verwerken van persoonsgegevens". Doet u niets met persoonsgegevens? Dan heeft u met de regels over privacy ook niet van doen. Maar geen enkel bedrijf doet niets met persoonsgegevens. Binnen bedrijven draait veel immers om mensen: er zijn mensen in dienst, mensen fungeren als contactpersonen van andere bedrijven met wie zaken wordt gedaan, mensen kopen uw producten of maken gebruik van uw diensten, enzovoort.

U vraagt zich misschien af wat er nu precies wordt bedoeld met de begrippen "persoonsgegeven" en "verwerken". Voor een goed begrip van deze serie over de AVG zullen wij een aantal van de belangrijkste termen hieronder weergeven en uitleggen.

> *Persoonsgegeven:* informatie over een geïdentificeerde of identificeerbare persoon. Informatie over een geïdentificeerde persoon is bijvoorbeeld: een naam en een adres. Een naam of vestigingsadres van een bedrijf is geen persoonsgegeven. Bij eenmanszaken en zzp'ers kan het vestigingsadres echter tevens het woonadres zijn. Dan is het weer wel een persoonsgegeven. Andere voorbeelden van persoonsgegevens: telefoonnummers (geen algemene bedrijfstelefoonnummers), e-mailadressen (info@-adressen zijn weer geen persoonsgegevens).
> Een persoon is identificeerbaar als je over een gegeven beschikt wat kan leiden tot identificatie van de desbetreffende persoon. Denk aan locatiegegevens, een burgerservicenummer of camerabeelden van een persoon. Al deze gegevens hebben betrekking op een identificeerbare persoon, omdat de gegevens in verband kunnen worden gebracht met een bepaalde persoon en op indirecte wijze identificatie mogelijk maken.
>
> *Verwerken*: een bewerking van een persoonsgegeven of een geheel van bewerkingen, zoals bijvoorbeeld opslaan, verzamelen, raadplegen, combineren, wissen, doorsturen, etc.
>
> *Betrokkene(n):*
> De persoon of personen van wie gegevens worden verwerkt.
>
> *Bijzondere persoonsgegevens:*
> dit zijn gegevens over ras, etnische afkomst, politieke opvatting, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, genetische of biometrische gegevens, gegevens over gezondheid, seksueel gedrag of seksuele gerichtheid.
>
> *Verwerkingsverantwoordelijke:* het bedrijf, de organisatie of de persoon/personen die bepaalt/bepalen waarvoor en hoe persoonsgegevens worden verwerkt.
>
> *Verwerker:* het bedrijf, de organisatie of de persoon/personen die de verwerking daadwerkelijk uitvoert/uitvoeren binnen het doel en met de middelen zoals de verwerkingsverantwoordelijke die heeft bepaald.

§ 1.2. Grondslagen

Eén van de hoofdregels binnen de privacywetgeving is dat u voor het mogen verwerken van persoonsgegevens een grondslag nodig heeft. Dat wil zeggen: er moet een legitieme reden zijn voor de verwerking. Deze grondslagen zijn opgesomd in de AVG:

1. De betrokkene heeft toestemming gegeven voor verwerking;
2. De verwerking is noodzakelijk in verband met het sluiten of de uitvoering van een overeenkomst;
3. De verwerking is noodzakelijk om een wettelijke verplichting uit te voeren;
4. De verwerking is noodzakelijk voor een vitaal belang van de betrokkene;
5. De verwerking is noodzakelijk voor de goede vervulling van een publiekrechtelijke taak;
6. De verwerking is noodzakelijk voor de behartiging van een gerechtvaardigd belang.

De voor een gemiddelde mkb'er meest relevante grondslagen zijn die genoemd onder punt 1, 2, 3 en 6.

Terug naar de checklist

§ 1.3 Algemene beginselen voor de verwerking van persoonsgegevens

Bij de verwerking van persoonsgegevens zijn een aantal algemene beginselen van belang. Persoonsgegevens mogen alleen worden verwerkt als daarbij de volgende uitgangspunten in acht worden genomen:

- Rechtmatigheid, behoorlijkheid en transparantie: u moet aan de wet voldoen en betrokkenen proactief informeren over de wijze waarop u hun persoonsgegevens verwerkt. De plicht om betrokkenen te informeren over de persoonsgegevens die u van hen verwerkt is een belangrijk onderdeel van de privacyregels.
- Doelbinding: de persoonsgegevens mogen alleen worden verwerkt voor vooraf vastgestelde en gespecificeerde doelen. De gegevens mogen niet voor andere doelen worden gebruikt.
- Minimale gegevensverwerking: alleen die gegevens die noodzakelijk zijn om het doel te bereiken mogen worden verwerkt.
- Juistheid: alle redelijke maatregelen moeten worden genomen om onjuiste gegevens te wissen of te corrigeren.
- Opslagbeperking: gegevens mogen niet langer worden bewaard dan noodzakelijk voor het doel.
- Integriteit en vertrouwelijkheid: de gegevens worden beveiligd door passende technische en organisatorische maatregelen te nemen.

Om aan de AVG-beginselen te voldoen is het handig om uw producten, diensten, systemen en programmatuur zo privacyvriendelijk mogelijk te laten zijn. Denk aan een CRM (*customer relationship management)*-systeem waarin standaard maar een beperkt aantal categorieën persoonsgegevens kan worden ingevuld. Of maak gebruik van software, zoals verzuimregistratie-software, die signaleert wanneer de bewaartermijn van persoonsgegevens verstrijkt. Dergelijke privacyvriendelijke maatregelen zijn niet alleen handig, de AVG schrijft zelfs voor dat u ze treft.

Over wat voor soort verwerking of welke categorie persoonsgegevens we het in deze serie ook hebben, u zult te allen tijde bovenstaande beginselen in acht moeten nemen. Daar waar wij u in deze serie adviezen geven, mag u er van uit gaan dat deze voldoen aan de genoemde beginselen.

Hoofdstuk 2: Beveiliging

§ 2.1 Passende maatregelen treffen

Verwerkt u persoonsgegevens, dan bent u verplicht om passende technische en organisatorische maatregelen te treffen om deze persoonsgegevens te beschermen. Het beveiligingsniveau moet zijn afgestemd op de risico's die verwerking met zich meebrengt. U kunt zich voorstellen dat een ziekenhuis aan strengere beveiligingseisen zal moeten voldoen dan een gemiddelde mkb'er. Dat heeft te maken met de activiteiten en de aard van de persoonsgegevens die daarbij worden verwerkt. Hoe gevoeliger de informatie die men verwerkt, hoe hoger de eisen die aan beveiliging worden gesteld.

Hoe ver men daarin precies moet gaan, hangt van allerlei omstandigheden af. Dat maakt dit onderwerp ook meteen zo lastig: het is niet mogelijk in zijn algemeenheid aan te geven waaraan uw beveiliging moet voldoen. Het hangt in ieder geval af van de volgende factoren:

1. De stand van de techniek;
2. De kosten voor het uitvoeren van de beveiligingsmaatregelen;
3. De aard van de persoonsgegevens;
4. De omvang van de persoonsgegevens;
5. De context waarbinnen de verwerking plaatsvindt;
6. De verwerkingsdoeleinden;
7. De risico's van verwerking, de waarschijnlijkheid en de ernst ervan.

De AVG probeert bovenstaande wat meer in te vullen door een viertal voorbeelden te noemen van belangrijke maatregelen die onderdeel van uw beveiliging zouden kunnen zijn. Of dit passend is, hangt van uw eigen specifieke situatie af:

1. Pseudonimisering en versleuteling van persoonsgegevens;
2. Maatregelen om de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van verwerkingssystemen en diensten te garanderen;
3. Maatregelen gericht op het tijdig kunnen herstellen van de beschikbaarheid van en de toegang tot persoonsgegevens bij een fysiek of technisch incident;
4. Het vaststellen van adequate procedures voor het periodiek evalueren van de doeltreffendheid van de genomen veiligheidsmaatregelen.

Het kan overigens ook zo zijn dat voor een deel van uw verwerkingen de risico's groter zijn en u voor dat deel strengere beveiligingsmaatregelen moet treffen dan voor andere verwerkingen. Denkt u bijvoorbeeld aan de loonadministratie. Bij de gemiddelde mkb'er zal dit deel beter beveiligd moeten zijn dan een klantadministratie die vooral uit NAW(naam-adres-woonplaats)-gegevens bestaat. Ook een bedrijf dat alleen aan andere bedrijven levert, zal aan minder hoge beveiligingseisen hoeven te voldoen dan een bedrijf dat alleen aan consumenten levert. Ook kan het beveiligingsniveau dat u nu heeft, over 10 jaar niet meer passend zijn. Het is dus een onderwerp dat blijvend uw aandacht moet krijgen.

Bij het treffen van maatregelen kunnen we verder een onderscheid maken tussen organisatorische en technische maatregelen. Hieronder zullen er voorbeelden van beide categorieën maatregelen worden genoemd:

Organisatorische maatregelen:

1. Het beperken van de personen die toegang hebben tot bepaalde persoonsgegevens: alleen de personen die de gegevens nodig hebben voor hun werk zouden toegang moeten hebben;
2. Het verlenen van toegang aan deze personen tot alleen die persoonsgegevens die zij nodig hebben voor hun werk en niet ook tot andere persoonsgegevens;
3. Het (schriftelijk) afspreken van geheimhouding met een boeteclausule met alle personen aan wie toegang tot persoonsgegevens zal worden verleend;
4. Het bewaren van persoonsgegevens op servers in afgesloten ruimtes;
5. Het bewaren van papieren dossiers in afgesloten kasten;
6. Het creëren van informatieveiligheidsbewustzijn onder medewerkers;
7. Het opstellen van duidelijke voorschriften en procedures voor het tijdig en doeltreffend behandelen van beveiligingsincidenten en zwakke plekken in de beveiliging;

8. Ervoor zorgen dat de voorschriften, procedures en wet- en regelgeving ook daadwerkelijk nageleefd worden.

Technische maatregelen:

1. Twee-factor-authenticatie (zoals dat bijvoorbeeld bij een e-mailaccount van Gmail kan worden ingesteld);
2. Logging (registreren welke activiteiten er zijn uitgevoerd met de persoonsgegevens en door wie);
3. Firewalls;
4. Virusscanners;
5. Software tegen malware-aanvallen;
6. Het periodiek maken van back-ups;
7. Software waarmee de verantwoordelijke of verwerker wordt geattendeerd op het dreigende verstrijken van een bewaartermijn.

Wij adviseren u in gesprek te gaan met uw ICT'er en om te bezien welke (technische) maatregelen in uw specifieke situatie al genomen zijn, of deze (voldoende) passend zijn en welke verdere maatregelen u eventueel nog zult moeten treffen.

Naar de checklist

§ 2.2 Datalekken

Vanaf 1 januari 2016 bestaat de meldplicht voor datalekken. Ook op grond van de AVG is er een meldplicht voor datalekken. Doet zich binnen uw bedrijf of bij één van uw verwerkers een datalek voor, dan bent u verplicht dat te melden bij de AP.

Van een datalek is sprake als er persoonsgegevens zijn vernietigd of verloren zijn gegaan, zijn gewijzigd, verstrekt of toegankelijk gemaakt op een manier die onrechtmatig is. Anders gezegd: Persoonsgegevens zijn in verkeerde handen gekomen. De meldplicht geldt echter alleen als het waarschijnlijk is dat het datalek een risico voor betrokkenen met zich meebrengt. Er kan zich een technisch of fysiek incident voordoen waarbij duidelijk is dat persoonsgegevens geen gevaar hebben gelopen. Zij zijn dan niet blootgesteld aan vernietiging, verlies, wijziging, etc., zodat er geen sprake is van een datalek. Hieronder tref u drie voorbeelden aan:

- Persoonsgegevens zijn opgeslagen op een usb-stick en deze stick wordt gestolen: dit is een datalek.
- Eén van uw werknemers laat een koffer met daarin persoonsgegevens achter in de trein. De koffer is voorzien van een goed slot en komt via 'gevonden voorwerpen' afgesloten weer bij u terug. Dit is géén datalek.
- Uitval van firewall: geen datalek.

Een datalek moet vaak ook worden gemeld aan diegenen wiens gegevens gelekt zijn, namelijk als het zeer waarschijnlijk is dat het lek negatieve gevolgen voor hen heeft. Het gaat dan om een datalek met een zogenaamd 'hoog risico'. Van een hoog risico is sprake als de te verwachten gevolgen van het datalek zich met grote waarschijnlijkheid voordoen. De kans dat die gevolgen zich verwezenlijken moet dus zeer waarschijnlijk zijn.

De termijn waarbinnen een datalek bij de AP moet worden gemeld is zéér kort: 72 uur na ontdekking. Ook als u nog niet alle feiten omtrent het datalek op een rijtje heeft, moet u de melding wel alvast doen.

Op dit moment heeft de AP nog geen nadere publicaties uitgebracht over de meldplicht datalekken zoals opgenomen in de AVG. Het lijkt er op dat de meldplicht datalekken onder de AVG (grotendeels) hetzelfde is als onder de Wbp. In ieder geval geldt wel een uitgebreidere documentatieplicht voor incidenten met persoonsgegevens, maar daarover gaat de volgende paragraaf. Er zit een publicatie van de AP over de meldplicht aan te komen, uiteraard komen wij bij u op dit onderwerp terug als er meer bekend is.

Doet zich een incident voor bij u en weet u niet of u dit moet melden of hoe u dat moet doen, neemt u dan contact op met Bedrijfsjuridisch Ledenadvies. Voor meer informatie over de meldplicht datalekken verwijzen wij u graag naar de huidige informatieve beleidsregels (versie 2015) die de AP hierover heeft opgesteld, te vinden via:
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

§ 2.3 Documentatieplicht voor incidenten

De AVG verplicht u om alle incidenten met persoonsgegevens te documenteren, dus niet alleen van incidenten die een meldplichtig datalek opleveren. Dit betekent dat u zult moeten bijhouden welke incidenten zich voordoen, wat de feitelijke situatie per incident is, onder welke omstandigheden zich een incident voordeed, de gevolgen daarvan en de corrigerende maatregelen die u eventueel heeft getroffen. U moet dit op verzoek aan de AP kunnen laten zien. Door ook de incidenten te documenteren die volgens u geen meldplichtig datalek zijn, wil de AP kunnen nagaan of u terecht niet heeft gemeld.

In bijlage 3 treft u een vragenlijst aan die u kunt gebruiken bij het documenteren van incidenten. Bij incidenten waarbij geen persoonsgegevens betrokken zijn, dan zult u al vrij snel klaar zijn. Als persoonsgegevens wel in gevaar zijn gekomen zult u meer vragen moeten doorlopen. De vragenlijst is gebaseerd op het formulier van de AP dat u op dit moment moet gebruiken bij het melden van een datalek. Is er dus sprake van een datalek dan is de informatie waar in deze bijlage naar wordt gevraagd de informatie die u minimaal aan de AP moet verstrekken. Overigens dateert het vragenformulier van december 2015. Mocht er eventueel een geupdatete versie beschikbaar worden gesteld door de AP, dan zullen wij dit deel van de serie AVG zo nodig aanpassen.

Naar de checklist

Hoofdstuk 3: De rechten van betrokkenen

Zoals wij eerder al aangaven, hebben betrokkenen onder de AVG meer rechten dan zij op grond van de Wbp hadden. U bent verplicht betrokkenen te informeren over hun rechten. Ook moet u in staat zijn om adequaat te kunnen reageren op een betrokkene die één van zijn rechten wenst uit te oefenen. Wij zullen achtereenvolgens de volgende rechten bespreken: inzage, rectificatie, wissing, beperking, overdraagbaarheid en bezwaar.

Er is ook nog het recht van betrokkenen om niet te worden onderworpen aan besluiten die de uitkomst van een computeranalyse zijn. Denk aan profilering (dit is het verzamelen, analyseren en combineren van (persoons)gegevens met als doel iemand in te delen in een bepaalde categorie), bepaalde geautomatiseerde verkeersboetes of beslissingen op AOW-aanvragen. Omdat dergelijke besluiten bij metaalbedrijf Jansen niet voorkomen, zullen wij dit recht verder niet behandelen.

§ 3.1 Termijn

Aan een verzoek van een betrokkene tot uitoefening van één van zijn rechten moet u in beginsel uiterlijk binnen één maand gehoor geven, maar als dat kan eerder. Ook moet u de betrokkene binnen deze termijn laten weten wat u met zijn verzoek heeft gedaan.

§ 3.2 Recht van inzage

De betrokkene mag u verzoeken om duidelijkheid te geven over het wel of niet verwerken van zijn persoonsgegevens. Als u netjes uw informatieverplichtingen bent nagekomen, zou een betrokkene hier in principe niet om hoeven vragen. Daarnaast mag de betrokkene u verzoeken om inzage in zijn gegevens (een kopie) en mag hij u vragen hem de volgende informatie te verstrekken:

a. Waarvoor zijn persoonsgegevens worden verwerkt (de doelen);
b. Welke (soort) persoonsgegevens worden verwerkt;
c. Aan wie u de persoonsgegevens doorgeeft;
d. Hoe lang u de persoonsgegevens bewaart of, indien het niet mogelijk is een concrete termijn te noemen: de criteria om die termijn te bepalen;
e. Dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken dat persoonsgegevens worden gecorrigeerd of gewist, of dat de verwerking van zijn persoonsgegevens wordt beperkt, en dat hij het recht heeft tegen die verwerking bezwaar te maken;
f. Dat de betrokkene het recht heeft een klacht in te dienen bij de toezichthoudende autoriteit (in Nederland de Autoriteit Persoonsgegevens);
g. Wanneer de persoonsgegevens niet bij de betrokkene worden verzameld: alle beschikbare informatie over de bron van die gegevens;
h. Indien gebruikt: het bestaan van geautomatiseerde besluitvorming (besluiten die de uitkomst zijn van een computeranalyse), inclusief profilering en nuttige informatie over de onderliggende logica, het belang en de verwachte gevolgen van die verwerking voor de betrokkene.
i. Geeft u persoonsgegevens door aan derde landen of internationale organisaties, dan heeft de betrokkene het recht in kennis te worden gesteld van de passende waarborgen die er in het land van bestemming zijn om zijn persoonsgegevens te beschermen.

Het geven van inzage in de persoonsgegevens die u verwerkt, komt in de praktijk vaak neer op het geven van een kopie aan de betrokkene. Als de betrokkene elektronisch om inzage verzoekt, mag u de informatie in een gangbare elektronische vorm aan de desbetreffende persoon verstrekken. U zou dit dus bijvoorbeeld in de vorm van een pdf-bestand kunnen toesturen.

§ 3.3 Recht op rectificatie

Een betrokkene mag u verzoeken om correctie van onjuiste persoonsgegevens en aanvulling van onvolledige gegevens. Bij het aanvullen van persoonsgegevens moet u wel in de gaten houden dat het geen persoonsgegeven betreft dat u niet nodig heeft voor het doel dat u met de verwerking van de persoonsgegevens nastreeft.

Terug naar de checklist

§ 3.4 Recht op wissing

De betrokkene mag u vragen om zijn persoonsgegevens te wissen. U moet hieraan in de volgende gevallen gehoor geven:

a. De persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij verzameld of verwerkt zijn;
b. De betrokkene trekt zijn eerder gegeven toestemming in en er is geen andere grondslag voor verwerking;
c. De betrokkene maakt bezwaar tegen verwerking en er zijn geen dwingende gerechtvaardigde gronden voor verwerking (bij direct marketing kan nooit sprake zijn van een dwingende gerechtvaardigde grond voor verwerking);
d. De persoonsgegevens zijn onrechtmatig, d.w.z. in strijd met de AVG, verwerkt;
e. De persoonsgegevens moeten worden gewist vanwege een wettelijke verplichting van de verwerkingsverantwoordelijke;
f. De persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij (hiermee wordt een mobieletelefonie of internetdienst bedoeld).

Er bestaan vijf uitzonderingen op het recht van de betrokkene op wissing van zijn persoonsgegevens, waarvan wij er hier twee zullen noemen. Wissing kan bijvoorbeeld worden geweigerd als op de verwerkingsverantwoordelijke een verwerkersverplichting rust (bijvoorbeeld de fiscale administratieplicht). Ook mag de verwerkingsverantwoordelijke wissing weigeren als hij de persoonsgegevens nodig heeft voor het instellen, uitoefenen of onderbouwen van een rechtsvordering. Denkt u daarbij aan de situatie dat u een klant, ter incassering van de openstaande vordering, wilt laten dagvaarden voor de burgerlijke rechter en de betrokkene plots om wissing verzoekt.

§ 3.5 Recht op beperking van de verwerking

Dit is het recht van een betrokkene om de verwerking van zijn persoonsgegevens tijdelijk stop te laten zetten, totdat een bepaald probleem of bezwaar is opgelost of weggenomen. De betrokkene mag hierom slechts in vier situaties verzoeken:

1. Betrokkene is van mening dat zijn persoonsgegevens niet juist zijn;
2. De verwerking van zijn gegevens is onrechtmatig (in strijd met de wet), maar de betrokkene wil niet dat zijn gegevens worden gewist;
3. De betrokkene heeft zijn persoonsgegevens nodig om een rechtsvordering in te stellen, uit te oefenen of te onderbouwen. Het zou dan niet handig zijn als de verantwoordelijke de persoonsgegevens wist. De verantwoordelijke mag er niets mee doen en zo kunnen de persoonsgegevens worden behouden bijvoorbeeld als bewijs.
4. Betrokkene heeft tegen de verwerking bezwaar gemaakt en de verwerkingsverantwoordelijke beslist hier niet onmiddellijk op. De beperking duurt dan totdat de verwerkingsverantwoordelijke op het bezwaar heeft beslist.

Zolang de beperking voortduurt, mogen de persoonsgegevens alleen worden opgeslagen. Opslag is ook een vorm van verwerking. Andere verwerkingen zijn niet toegestaan. Een beperking van verwerking kan alleen nog worden opgeheven met toestemming van de betrokkene. Ook kan de beperking worden opgeheven als de verwerkingsverantwoordelijke de persoonsgegevens zelf nodig heeft voor een rechtsvordering. Ook de bescherming van de rechten van een ander of algemene gewichtige redenen kunnen maken dat de beperking van de verwerking moet worden opgeheven.

§ 3.6 Recht op overdraagbaarheid

Dit recht is nieuw en bestond niet onder de Wbp. Het recht houdt in dat betrokkenen mogen verzoeken om hen een digitale kopie van hun persoonsgegevens te verstrekken, die zij ten behoeve van een andere partij kunnen gebruiken. Ook kunnen mensen vragen om hun persoonsgegevens rechtstreeks over te dragen aan een andere organisatie. Het bestand dat u moet verstrekken dient ‘gestructureerd, gangbaar en in machinaal leesbare vorm’ te zijn. Het meest eenvoudige voorbeeld is om de persoonsgegevens in een Excel-bestand aan de betrokkene te verstrekken.

De verwerkingsverantwoordelijke moet de persoonsgegevens verstrekken die de betrokkene actief en bewust aan u heeft verstrekt. Denk aan de accountgegevens (e-mailadres, gebruikersnaam, leeftijd etc.) die zij op een online formulier hebben ingevuld. U moet echter ook de gegevens verstrekken die de betrokkene min of meer onbewust aan u heeft verstrekt door uw product of dienst te gebruiken. Denk hierbij aan de persoonsgegevens die worden verzameld door gebruik te maken van uw website (cookies). Verder moet de verwerkingsverantwoordelijke niet alleen de persoonsgegevens zelf verstrekken, maar ook de metagegevens. Metagegevens zijn gegevens over de persoonsgegevens, zoals tijdstip, afzender, geadresseerde etc.

Het recht op overdraagbaarheid bestaat alleen als persoonsgegevens worden verwerkt op grond van toestemming van de betrokkene of omdat verwerking noodzakelijk is voor de uitvoering van een overeenkomst (zie § 1.2 van dit deel over de grondslagen voor verwerking). In andere gevallen hebben betrokkenen geen recht op overdraagbaarheid. Is er sprake van een andere grondslag voor de verwerking van persoonsgegevens, dan kan de betrokkene wel een beroep doen op zijn recht op inzage, in het kader waarvan u alsnog een kopie van zijn gegevens moet verstrekken. Aan de eis van 'gestructureerd, gangbaar en in machinaal leesbare vorm' hoeft deze kopie dan echter niet te voldoen.

Tot slot bestaat het recht op overdraagbaarheid alleen als er sprake is van geheel geautomatiseerde verwerking. Wij verwachten dat de meeste Metaalunieleden persoonsgegevens zullen verwerken met behulp van de computer, zodat aan deze eis is voldaan.

§ 3.7 Recht van bezwaar

Personen wiens gegevens worden verwerkt mogen daartegen bezwaar maken. Dat kan alleen als verwerking plaatsvindt op basis van de grondslagen: "taak van algemeen belang" en "gerechtvaardigd belang". Bij deze grondslagen moet de verwerkingsverantwoordelijke immers, voordat hij tot verwerking van persoonsgegevens overgaat, een afweging maken tussen de belangen van hemzelf en die van de betrokkene. Tegen de uitkomst van die belangenafweging kan het bezwaar zich richten. Er zal dan dus vaak sprake zijn van een situatie die maakt dat de betrokkene zich niet kan vinden in verwerking van zijn persoonsgegevens. Deze situatie zorgt er dan voor dat de belangenafweging anders uit moet vallen en verwerking toch gestaakt moet worden.

Bij de andere grondslagen die basis kunnen zijn voor het verwerken van persoonsgegevens speelt het recht van bezwaar niet. Als u persoonsgegevens verwerkt om een overeenkomst uit te kunnen voeren, zou het immers vreemd zijn als de betrokkene het met verwerking niet eens is.

Als u als verwerkingsverantwoordelijke een bezwaar ontvangt, gaat u dan eerst na welke grondslag de basis is voor verwerking van de persoonsgegevens van degene van wie het bezwaar afkomstig is. Is er sprake van een taak van algemeen belang of een gerechtvaardigd belang, dan bent u in principe verplicht te stoppen met verwerking van de persoonsgegevens. Alleen als er sprake is van dwingende gerechtvaardigde belangen die zwaarder wegen dan de belangen, grondrechten of fundamentele vrijheden van de betrokkene mag u het bezwaar naast u neer leggen.

Maakt de betrokkene bezwaar tegen direct marketing, dan bent u altijd verplicht om aan dit bezwaar gehoor te geven en te stoppen met verdere verwerking van persoonsgegevens voor dit doel. U mag dan geen commerciële berichten meer toesturen en u zult de persoonsgegevens moeten wissen/verwijderen, tenzij u de persoonsgegevens uiteraard nog voor andere doelen moet bewaren.

§ 3.8 In kennis stellen van derden over uitoefening rechten

Als een betrokkene het recht op rectificatie, wissing of beperking uitoefent, is het belangrijk dat u eventuele derden aan wie de desbetreffende persoonsgegevens zijn doorgegeven hiervan op de hoogte worden gesteld. Stel dat een betrokkene om rectificatie verzoekt, dan moet ook de partij die deze gegevens van u heeft ontvangen tot correctie overgaan.

Hoofdstuk 4: De functionaris voor gegevensbescherming

Een ander onderdeel van de AVG gaat over de functionaris voor gegevensbescherming, kortweg "FG" genoemd. Sommige bedrijven zullen iemand moeten aanstellen die als functionaris voor gegevensbescherming zal gaan optreden. Zo'n FG moet het bedrijf en diens werknemers adviseren en informeren over de verplichtingen van de AVG en toezien op de naleving daarvan. Een FG is in de volgende gevallen verplicht:

1. U bent een overheidsinstantie of overheidsorgaan (rechterlijke macht uitgezonderd);
2. U houdt zich voornamelijk bezig met het op grote schaal regelmatig en stelselmatig observeren van personen;
3. U houdt zich voornamelijk bezig met grootschalige verwerking van bijzondere persoonsgegevens en persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten.

Over het algemeen zal het voor u wel helder zijn of u onder nummer 1 valt. Er zullen naar alle waarschijnlijkheid geen Metaalunieleden zijn die tot de overheid behoren. Om te beoordelen of u valt onder nummer 2 of 3 hierboven, moet u uw kernactiviteiten als uitgangspunt nemen. Dat zijn alle processen die essentieel zijn om de bedrijfsdoelstellingen te (kunnen) realiseren, of de processen die tot de hoofdtaken van uw bedrijf horen. U zult zich dan dus moeten afvragen of het op grote schaal regelmatig en stelselmatig observeren van personen of het grootschalig verwerken van bijzondere en strafrechtelijke persoonsgegevens tot uw kernactiviteiten behoort. De meeste Metaalunieleden zullen deze vraag met een "nee" kunnen beantwoorden, wat betekent dat zij niet verplicht zijn een FG aan te stellen.

Nederland heeft de vrijheid om in aanvullende wetgeving te bepalen dat in meer gevallen dan hierboven genoemd een FG moet worden aangesteld. Het is bij de publicatie van deze uitgave nog onbekend of Nederland gebruik gaat maken van die mogelijkheid.

Naar de checklist.

Hoofdstuk 5: De gegevensbeschermingseffectbeoordeling

De AVG schrijft voor dat in sommige gevallen een gegevensbeschermingseffectbeoordeling moet worden uitgevoerd. Dit wordt ook wel de data protection impact assessment (DPIA) genoemd. Het is in feite een rapportage van een beoordeling die u heeft gemaakt over een verwerking die u wilt gaan uitvoeren, de risico's die die verwerking met zich meebrengt en de getroffen maatregelen om de risico's te beperken.

Een DPIA is alleen verplicht als een verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van personen. Hier is het weer de vraag wanneer je van verwerkingen met een hoog risico kunt spreken. U moet dit in principe zelf beoordelen, de AVG vult dit niet concreet in. De Europese privacytoezichthouders hebben wel aangegeven dat u als vuistregel kunt hanteren dat u een DPIA moet uitvoeren als uw verwerking aan 2 of meer van de onderstaande 9 punten voldoet:

1. U beoordeelt mensen op basis van persoonskenmerken (voorbeeld: een bedrijf dat bezoekers van zijn website volgt en op basis daarvan profielen van deze mensen opstelt).

2. U neemt geautomatiseerde beslissingen die voor de betrokkene rechtsgevolgen of vergelijkbare wezenlijke gevolgen hebben (voorbeelden: geautomatiseerde verkeersboetes, geautomatiseerde beslissingen van overheidsinstanties, zoals de Sociale Verzekeringsbank die op een AOW-aanvraag beslist).

3. U houdt zich bezig met stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten, bijvoorbeeld met cameratoezicht.

4. U verwerkt gevoelige persoonsgegevens (het gaat hierbij om bijzondere categorieën van persoonsgegevens, maar ook om gegevens die over het algemeen als privacygevoelig worden beschouwd, zoals gegevens over elektronische communicatie, locatiegegevens en financiële gegevens).

5. U houdt zich bezig met grootschalige gegevensverwerkingen. Of verwerkingen grootschalig zijn, hangt af van de hoeveelheid mensen van wie gegevens worden verwerk, de hoeveelheid gegevens en/of de verscheidenheid aan gegevens die worden verwerkt, de tijdsduur van de gegevensverwerking en de geografische reikwijdte van de gegevensverwerking.

6. U combineert databases met persoonsgegevens met elkaar of koppelt databases met gegevens aan elkaar.

7. U verwerkt persoonsgegevens over kwetsbare personen (er is vaak sprake van een ongelijke machtsverhouding tussen u en de betrokkene. Denk aan werknemers, kinderen en patiënten).

8. U maakt gebruik van nieuwe technologieën (bijvoorbeeld vingerafdruksystemen en gezichtsherkenning t.b.v. toegangscontrole, een automatic numberplate recognition camera of "internet of things" applicaties die een grote impact kunnen hebben op het dagelijks leven en de privacy van mensen).

9. De verwerking van persoonsgegevens kan leiden tot het niet kunnen uitoefenen van een recht, het niet gebruik kunnen maken van een dienst of het niet kunnen afsluiten van een contract (voorbeelden: gegevensverwerkingen die plaatsvinden in de openbare ruimte en die mensen niet kunnen vermijden, een bank die de kredietwaardigheid van klanten toetst om te bepalen of zij een lening krijgen).

Bovenstaande laat onverlet dat ook in andere gevallen waarbij de verwerking waarschijnlijk een hoog risico oplevert, een DPIA verplicht is. De AP zal op termijn een lijst publiceren van verwerkingen waarvoor in ieder geval een DPIA verplicht is.

Is een DPIA in uw geval verplicht, dan moet u de voorgenomen verwerkingen beoordelen op de volgende aspecten:

1. De gegevens die u wilt gaan verwerken en het doel van de verwerking;

2. Als een gerechtvaardigd belang uw grondslag voor verwerking is, moet u ook het belang of de belangen benoemen;
3. De noodzaak van de verwerking op de manier zoals u dat wilt gaan doen (kan het niet op een manier die minder inbreuk maakt op de privacy);
4. Of de inbreuk op de privacy wel in verhouding staat tot het doel dat u met de verwerking wilt bereiken;
5. Welke risico's de verwerking met zich meebrengt voor de betrokkenen;
6. Welke maatregelen u gaat nemen om de risico's te voorkomen/beperken en wat u gaat doen om aan te tonen dat u aan de AVG voldoet.

De bovenstaande beoordeling zult u schriftelijk moeten vastleggen.

Wilt u meer in detail weten hoe u een DPIA moet uitvoeren? Voor een handreiking voor de uitvoering verwijst de AP zelf naar de beroepsorganisatie van IT-auditors: https://www.norea.nl/download/?id=522.

Ten aanzien van de gemiddelde mkb'er schatten wij in dat bij de administratieve onderdelen uit deze serie vaak niet aan twee of meer van bovenstaande criteria zal zijn voldaan. Omdat wij een zeer gevarieerde achterban hebben en alleen u weet welke verwerkingen u uitvoert, blijft het van groot belang zelf te bekijken of een DPIA al dan niet verplicht is. Twijfelt u of u verwerkingen uitvoert met waarschijnlijk een hoog risico, neemt u dan contact met ons op. Verder zullen wij u op de hoogte stellen zodra de AP haar lijst met verwerkingen heeft gepubliceerd waarvoor in ieder geval een DPIA is verplicht.

Naar de checklist

Hoofdstuk 6: Het doorgeven van persoonsgegevens aan derden

Wanneer u als bedrijf persoonsgegevens van iemand ontvangt, kan het nodig of wenselijk zijn om deze gegevens door te geven aan een andere partij. Met doorgifte van persoonsgegevens aan andere partijen zult u zeer voorzichtig moeten zijn. Het doorgeven van persoonsgegevens aan een ander is een vorm van verwerking, zodat u dus aan de regels uit de AVG moet voldoen.

Bij de doorgifte van persoonsgegevens aan derden wordt een onderscheid gemaakt in het land van bestemming waar de persoonsgegevens naartoe gaan:

1. De ontvanger van de persoonsgegevens zit in de EER[2];
2. De ontvanger zit buiten de EER.

Ten aanzien van doorgifte van persoonsgegevens aan een entiteit in een land binnen de EER zult u alle van toepassing zijnde regels uit de AVG over het omgaan met persoonsgegevens moeten naleven. Ook op de verwerking(en) door de ontvanger is de AVG van toepassing. Voor doorgifte moet dan in ieder geval een grondslag bestaan, zoals omschreven in § 1.2 van dit algemene deel en u moet de betrokkenen vooraf over de doorgifte informeren.

Doorgifte van persoonsgegevens aan landen buiten de EER is aan strengere eisen onderworpen. Dat komt omdat de AVG de privacy in heel Europa regelt en het beschermingsniveau in de gehele EER daardoor in principe hetzelfde is. Buiten de EER is de bescherming echter wellicht minder goed geregeld.

Doorgifte aan een land buiten de EER is slechts toegestaan als dat land passende waarborgen biedt voor de bescherming van persoonsgegevens. Dat kan bijvoorbeeld blijken uit een besluit van de Europese Commissie, die in dat besluit verklaart dat het ontvangende land een adequaat beschermingsniveau heeft[3]. Met adequaat wordt dan bedoeld: vergelijkbaar met de EER. Zo'n besluit wordt een adequaatheidsbesluit genoemd.

Is er geen adequaatheidsbesluit, dan mag doorgifte alleen als er op een andere manier passende waarborgen zijn voor de bescherming van de persoonsgegevens. De passende waarborgen kunnen bijvoorbeeld zijn neergelegd in een modelcontract (tussen u en de ontvanger) dat is goedgekeurd door de Europese Commissie. Er zijn op dit moment drie modelcontracten beschikbaar. U kunt deze modelcontracten raadplegen via de website van de AP: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-binnen-en-buiten-de-eu. Kijkt u onder "Vragen over doorgifte naar derde landen" onder de vraag "Welke modelcontracten zijn er voor doorgifte naar een derde land". Gebruikt u zo'n modelcontract zonder aanvullingen of wijzigingen, dan is doorgifte toegestaan.

U mag ook zelf contractsbepalingen opstellen, maar deze zullen dan wel vooraf moeten worden goedgekeurd door de toezichthoudende instantie (de AP). Er zijn nog een aantal mogelijkheden om persoonsgegevens te mogen doorgeven, maar het voert te ver die hier allemaal te bespreken.

Op de regel dat u alleen persoonsgegevens mag doorgeven aan een land of organisatie buiten de EER dat een passend beschermingsniveau biedt, bestaan een aantal uitzonderingen. De drie belangrijkste uitzonderingen zijn:

1. De betrokkene heeft uitdrukkelijk met doorgifte ingestemd;
2. Doorgifte is noodzakelijk voor de uitvoering van een overeenkomst tussen de verwerkingsverantwoordelijke en de betrokkene of is noodzakelijk voor de uitvoering van – op verzoek van de betrokkene – genomen precontractuele maatregelen.
3. Doorgifte is noodzakelijk voor de sluiting of uitvoering van een overeenkomst in het belang van de betrokkene, maar die is gesloten tussen de verwerkingsverantwoordelijke en een ander.

Er valt nog veel meer te zeggen over doorgifte van persoonsgegevens aan derden. Het voert echter te ver om alle ins en outs hier te behandelen. Heeft u vragen over doorgifte van persoonsgegevens aan derden, neemt u dan contact met ons op.

---

[2] EER: alle landen van de EU plus Liechtenstein, Noorwegen en IJsland.

[3] Zie htttp://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm voor een overzicht van de landen waarvoor een adequaatheidsbesluit is genomen.

Hoofdstuk 7: Het register voor verwerkingsactiviteiten

§ 7.1 Wat houdt de registratieplicht in

Op grond van de AVG is het in beginsel verplicht om een register bij te houden van alle verwerkingsactiviteiten die onder uw verantwoordelijkheid plaatsvinden. Dit heeft tot doel om aan te kunnen tonen dat u aan de AVG voldoet. In het verwerkingsregister moeten de volgende gegevens worden opgenomen:

1. De naam en contactgegevens van verantwoordelijke (of diens vertegenwoordiger, wanneer de verantwoordelijke buiten de EER[4] is gevestigd), en van de functionaris voor gegevensbescherming (indien aanwezig);
2. De doeleinden waarvoor gegevens worden verwerkt;
3. De categorieën persoonsgegevens (zoals NAW-gegevens, contactgegevens, betaalgegevens);
4. De categorieën betrokkenen (bijvoorbeeld: klanten, websitebezoekers, werknemers);
5. De categorieën ontvangers (aan wie worden de gegevens verstrekt?);
6. Informatie over eventuele doorgifte van gegevens naar landen buiten de EER;
7. De bewaartermijnen van de gegevens;
8. De manieren waarop gegevens zijn beveiligd (bijvoorbeeld: encryptie, logische toegangscontrole, pseudonimisering).

Maakt u gebruik van een verwerker, dan zal ook deze partij een register moeten bijhouden. Het register van de verwerker heeft dan betrekking op de verwerkingen die hij onder uw verantwoordelijkheid uitvoert. Verwerkers registreren:

1. De naam en contactgegevens van de verwerker en de verantwoordelijke (of hun vertegenwoordigers) en (indien aanwezig) de functionaris voor gegevensbescherming;
2. De categorieën verwerkingen (dit komt overeen met de doeleinden uit het register van de verantwoordelijke);
3. Informatie over eventueel doorgifte van gegevens naar landen buiten de EER;
4. De manieren waarop gegevens zijn beveiligd.

§ 7.2 Uitzonderingen op de registratieplicht

Het bijhouden van een register voor de verwerkingsactiviteiten is niet in alle gevallen verplicht. Ondernemingen of organisaties die minder dan 250 personen in dienst hebben hoeven hieraan niet te voldoen. In wezen is dit een mkb uitzondering, maar de meeste mkb'ers zullen waarschijnlijk toch weinig profijt gaan hebben van deze uitzondering. In drie gevallen kan men namelijk toch geen beroep doen op de hiervoor aangehaalde uitzondering:

1. U voert risicovolle verwerkingen uit;
2. U verwerkt bijzondere of strafrechtelijke persoonsgegevens;
3. U verwerkt persoonsgegevens op structurele basis.

Het eerste punt hierboven zal voor de gemiddelde mkb'er niet aan de orde zal zijn. Voor het mkb zullen de punten 2 en 3 het meest van belang zijn. In het kader van de personeels- en loonadministratie worden in de meeste gevallen bijzondere persoonsgegevens verwerkt. Ten aanzien van punt 3 is de vraag natuurlijk wanneer een verwerking als incidenteel dan wel structureel moet worden beschouwd. Helaas is dat bij het verschijnen van dit deel nog niet duidelijk. Wel achten we de kans zeer groot dat bij de meeste mkb'ers verwerkingen van structurele aard voorkomen. Een klant- en leveranciersadministratie en een personeels- en loonadministratie hebben immers niet bepaald een incidenteel karakter. Verwerkingen hierbinnen vinden continu plaats. De in de AVG opgenomen uitzondering voor het mkb op de registratieplicht heeft dus waarschijnlijk in de praktijk nauwelijks waarde.

§ 7.3 Hoe te voldoen aan de registratieplicht

[4] EER: alle landen van de EU plus Liechtenstein, Noorwegen en IJsland.

Om aan de AVG te voldoen, adviseren wij u om al uw verwerkingsactiviteiten te registreren. U zult er uiteraard ook voor moeten zorgen dat het register actueel wordt gehouden. Dat betekent dat u ook wijzigingen moet bijhouden. Komt er een verwerking bij, vul het register dan aan. Valt er een verwerking af, verwijder deze dan weer, etc. U doet er verstandig aan na iedere wijziging het register onder een nieuwe naam op te slaan of om een nieuw (gedateerd) exemplaar uit te printen. Het is verstandig om binnen uw bedrijf een procedure in het leven te roepen voor het actueel houden van het register.

In bijlage 4 treft u een voorbeeld van een verwerkingsregister aan. U kunt de inhoud van het voorbeeldregister overnemen in een Excel-bestand. Het is ook mogelijk een kant-en-klaar Excel bestand bij ons op te vragen waarmee u uw verwerkingen eenvoudig kunt bijhouden. Wilt u dit sheet ontvangen, neemt u dan contact op met het secretariaat Bedrijfsjuridisch Ledenadvies: 030-6053344 of via bj@metaalunie.nl. Het register is ook te downloaden op onze website via www.metaalunie.nl/avg/downloads

Naar de checklist

Hoofdstuk 8: Verantwoordingsplicht ('accountability')

Het is verplicht om op verzoek van de AP te laten zien dat u aan de AVG voldoet. Concreet betekent dit dat u moet gaan opschrijven welke maatregelen u heeft genomen om dit doel te bereiken.

In de eerste plaats zult u dus een overzicht moeten maken van uw gegevensverwerkingen. U zult ten minste moeten documenteren welke categorieën van gegevens u verwerkt, waar die gegevens vandaan komen, met wie u ze deelt en welke grondslagen u voor uw verwerkingen gebruikt. Een groot deel van deze informatie moet u ook al opnemen in uw register voor verwerkingsactiviteiten, dus daar beschikt u dan al over.

Wij begrijpen dat het wellicht lastig is om concreet invulling te geven aan uw verantwoordingsplicht. Om die reden adviseren wij u om per type verwerking de actiepuntenlijst uit te voeren en als hoofddocument te gebruiken ter onderbouwing van uw verantwoordingsplicht. Voor elk punt dat u heeft uitgevoerd maakt u - indien nodig - een bijlage. In die bijlagen schrijft u precies op hoe u het desbetreffende actiepunt in de praktijk heeft uitgewerkt. Documenteert u ook waarom u vindt dat u ten aanzien van een bepaald onderwerp juist geen actie hoeft te ondernemen (bijvoorbeeld: schrijf op waarom uw bedrijf volgens u géén FG hoeft aan te stellen).

Let u erop dat de actiepuntenlijst is gebaseerd op wat metaalbedrijf Jansen doet. Voor zover u dus verwerkingen uitvoert die metaalbedrijf Jansen niet uitvoert, dient u het document aan te vullen.

Naar de checklist

DEEL 2: PERSONEELS- EN LOONADMINISTRATIE

Hoofdstuk 1: Het profiel van metaalbedrijf Jansen t.a.v. personeels- en loonadministratie

Hieronder zullen de kenmerken worden geschetst van metaalbedrijf Jansen, een door ons bedacht bedrijf dat zoveel mogelijk model staat voor en overeenkomsten heeft met de gemiddelde mkb'er. Voldoet u aan het geschetste profiel van metaalbedrijf Jansen, dan is dit deel uit deze serie integraal op u van toepassing en moet u – om aan de AVG te voldoen – de actiepuntenlijst volledig uitvoeren.

In dit deel van de serie over de AVG gaat het zoals aangegeven over de personeels- en loonadministratie**.** Hieronder verstaan wij alle bestanden, toepassingen en programma's die betrekking hebben op de administratie van personeels- en salarisgegevens van werknemers.

Let op: Alle natuurlijke personen die zich in een vergelijkbare positie bevinden als werknemers, genieten dezelfde bescherming. Voor de leesbaarheid van de tekst zullen wij hierna telkens over 'werknemers' spreken, maar hieronder moet, tenzij anders aangegeven, uitdrukkelijk worden verstaan: sollicitanten, werknemers, stagiaires, ex-werknemers, uitzendkrachten, payroll-werknemers of andere tijdelijke ingehuurde arbeidskrachten.

Metaalbedrijf Jansen heeft de hieronder genoemde kenmerken. Als u dat gemakkelijk vindt, kunt u ieder kenmerk uit het profiel voor uzelf afvinken door het opsommingsteken aan te kruisen.

- ○ Metaalbedrijf Jansen heeft werknemers in dienst (op basis van een arbeidsovereenkomst voor bepaalde of onbepaalde tijd) en/of werkt met uitzendkrachten/payroll-werknemers en stagiaires.

- ○ De persoonsgegevens hebben betrekking op werknemers, waaronder in dit geval dus moet worden verstaan: sollicitanten, werknemers, stagiaires, ex-werknemers, uitzendkrachten en payroll-werknemers.

- ○ De persoonsgegevens zijn afkomstig van de werknemers zelf, metaalbedrijf Jansen heeft ze niet van derden verkregen, tenzij sprake is van een uitzendkracht.

- ○ Metaalbedrijf Jansen verwerkt persoonsgegevens op geautomatiseerde wijze, wat wil zeggen dat zij met behulp van één of meer computers persoonsgegevens opslaat, bewerkt, etc. Met andere woorden: de personeels- en loonadministratie wordt digitaal beheerd.

- ○ Metaalbedrijf Jansen verwerkt ook bijzondere persoonsgegevens (dit zijn gegevens over ras, etnische afkomst, politieke opvatting, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, genetische of biometrische gegevens, gegevens over gezondheid, seksueel gedrag of seksuele gerichtheid).

- ○ Metaalbedrijf Jansen maakt gebruik van Microsoft Windows of Microsoft Office.

- ○ Metaalbedrijf Jansen besteedt de personeelsadministratie niet uit aan een externe personeelsafdeling of -dienst. Wel verstrekt zij de persoonsgegevens van haar werknemers aan een externe loonadministrateur, boekhouder of accountant ten behoeve van uitvoering van de loonadministratie. Daarnaast werkt metaalbedrijf Jansen samen met de arbodienst, het pensioenfonds, de verzuimverzekeraar en leasemaatschappij.

- ○ De gegevens worden niet gekoppeld aan of samengevoegd met andere gegevens van de werknemers die op een ander moment en/of in een andere context zijn verkregen, waardoor metaalbedrijf Jansen nog meer weet van de desbetreffende werknemers.

- ○ Bij de verwerking van persoonsgegevens maakt zij verder geen gebruik van (volledig) nieuwe technologie (bijv. vingerafdruksystemen of gezichtsherkenning). Doet u dat wel,

dan moet u mogelijk een gegevensbeschermingseffectbeoordeling uitvoeren. Zie hoofdstuk 5 van het algemene deel voor meer informatie.

○ Zij stelt met behulp van de persoonsgegevens geen profielen op van de betrokkenen om een beeld te krijgen van bijvoorbeeld hun interesses, gedrag, economische situatie etc.

○ Opslag van persoonsgegevens bij metaalbedrijf Jansen vindt plaats op de harde schijf van de eigen computer(s) en bij haar zelf aanwezige extra schijfruimte.

○ Metaalbedrijf Jansen maakt daarnaast gebruik van de diensten van een hosting-/cloudprovider. Deze provider levert opslagruimte en host de bedrijfswebsite en e-mail.

Hoofdstuk 2: Lijst van actiepunten

Indien u voldoet aan het geschetste profiel van metaalbedrijf Jansen, dan kunt u onderstaande actiepunten uitvoeren om t.a.v. de personeels- en loonadministratie aan de Algemene Verordening Gegevensbescherming te voldoen.

Vindplaats toelichting	Actiepunten	Uitgevoerd
PERSONEELS- EN LOONADMINISTRATIE (profiel metaalbedrijf Jansen, zie hoofdstuk 1 van deel 2)		
Hfd. 4 (alg deel)	Ga na of u een functionaris voor gegevensbescherming moet aanstellen. Dit actiepunt hoeft u niet uit te voeren als u dit al had gedaan in het kader van de vorige checklist (klant- en leveranciersadministratie).	
Hfd. 5 (alg deel)	Ga na of er verwerkingen binnen uw personeels- en loonadministratie plaatsvinden waarvoor u een DPIA (een gegevensbeschermingseffectbeoordeling) moet uitvoeren.	
§ 1.2 (alg deel) en § 3.2 (deel 2)	Beoordeel of de verwerkingen die u uitvoert berusten op één van de wettelijke grondslagen (let daarbij op het probleem met de grondslag 'toestemming'!) en ga na of u gebruikmaakt of wil maken van monitoring van werknemers. Vraagt u zich in dat geval het volgende af: - Is hiervoor een gerechtvaardigd belang aanwezig? Zo ja, welk belang?; - Weegt dit belang redelijkerwijs zwaarder dan het (privacy)belang van de werknemer?; - Is de vorm van monitoring noodzakelijk om uw doel te bereiken of kan dit doel ook op minder ingrijpende wijze worden bereikt?; - Leg de uitkomst van uw afweging schriftelijk vast; en - Ga na of de OR instemming heeft verleend.	
§ 3.3 en § 3.3.1 (deel 2)	Inventariseer welke bijzondere gegevens u verwerkt aan de hand van de uitleg en voorbeelden uit paragraaf 3.3 en 3.3.1.	
§ 3.3.2 en § 3.3.3 (deel 2)	Ga na of u zich ten aanzien van de verwerkingen van bijzondere persoonsgegevens kunt beroepen op één van de uitzonderingsgronden zoals genoemd in de AVG of de Uitvoeringswet AVG. Zie hiervoor paragraaf 3.3.2 en § 3.3.3.	
§ 3.4 (deel 2)	Stel een privacyverklaring op waarin u uw werknemers (waaronder wij in dit geval ook verstaan sollicitanten, stagiaires, ex-werknemers, uitzendkrachten/payroll-werknemers of andere tijdelijke ingehuurde arbeidskrachten) informeert over de onderwerpen waarover u hen moet informeren. U kunt hiervoor de onderstaande tekst gebruiken: **...Uw naam (incl. rechtsvorm) vestigingsadres...** **...postcode, plaats...** **...telefoonnummer en e-mailadres...** ***Verzamelen en gebruiken van persoonsgegevens van sollicitanten, uitzendkrachten/payroll-werknemers, stagiaires en werknemers*** *Graag maken wij u er op attent dat wij de persoonsgegevens die u ons verstrekt zullen verzamelen en gebruiken omdat dit noodzakelijk is voor het doorlopen van de sollicitatieprocedure of om een (eventuele) arbeidsovereenkomst / stageovereenkomst / uitzendovereenkomst te sluiten en uit te voeren. Daarnaast zijn bepaalde persoonsgegevens nodig voor de nakoming en uitvoering van bepalingen uit de voor ons geldende CAO. Ook verzamelen en gebruiken wij uw persoonsgegevens om aan bepaalde wettelijke verplichtingen te kunnen voldoen. Deze wette-*	

lijke verplichtingen hebben bijvoorbeeld te maken met de vaststelling en verschuldigdheid van belastingen en premies voor werknemers.

Gelet op deze noodzaak bent u verplicht om de hiervoor benodigde persoonsgegevens aan ons te verstrekken. Als u ons geen of onvoldoende persoonsgegevens verstrekt, dan kunnen wij mogelijk geen sollicitatieprocedure met u doorlopen, een (eventuele) arbeidsovereenkomst / stageovereenkomst / uitzendovereenkomst met u aangaan en uitvoeren of aan onze wettelijke verplichtingen voldoen.

Bent u (payroll-)werknemer of stagiair, dan gebruiken wij uw gegevens voor het opstellen, uitvoeren en beëindigen van de arbeids- of stageovereenkomst of de arbeidsrelatie. Hieronder wordt onder meer verstaan:

a) de behandeling van personeelszaken;
b) het vaststellen en uitbetalen van het salaris, vergoedingen en andere geldbedragen; en
c) het vaststellen en betalen van eventuele belastingen, premies en andere fiscale verplichtingen ten behoeve van u als werknemer of stagiair.

Bent u een sollicitant, dan gebruiken wij uw gegevens om met u te kunnen communiceren over het verloop van de sollicitatieprocedure, de beoordeling van uw geschiktheid voor een functie die vacant is of kan komen en de eventuele afhandeling van de door u gemaakte onkosten.

Bent u een uitzendkracht, dan zullen wij de gegevens die wij verkrijgen van het uitzendbureau gebruiken voor de beoordeling van uw geschiktheid voor een functie die vacant is of kan komen en voor de uitvoering van de uitzendovereenkomst.

Doorgifte aan derden
*Het is mogelijk dat wij uw persoonsgegevens doorgeven aan andere partijen. Deze andere partijen kunnen overheidsorganen zijn, maar ook partijen die in onze opdracht werkzaamheden uitvoeren of partijen aan wie wij verplicht zijn gegevens te verstrekken in verband met de (uitvoering van de) arbeidsovereenkomst. Het gaat om de volgende partijen: [**graag verder aanvullen of aanpassen**]*

- *de Belastingdienst;*
- *het UWV;*
- *onze arbodienst/bedrijfsarts;*
- *de Inspectie voor Sociale Zaken en Werkgelegenheid;*
- *het Pensioenfonds;*
- *de leasemaatschappij;*
- *de verzuimverzekeraar;*
- *onze accountant/boekhouder/salarisadministrateur;*
- *[…]*
- *[…]*

Soms zal het verstrekken van uw gegevens aan een ander noodzakelijk zijn om te kunnen voldoen aan de wet, zoals het geval is bij doorgifte aan de Belastingdienst, het UWV, de arbodienst/bedrijfsarts, het (verplicht gestelde) Pensioenfonds en de Inspectie voor Sociale Zaken en Werkgelegenheid.

In andere gevallen is de doorgifte noodzakelijk om de (arbeids)overeenkomst met u te kunnen uitvoeren, zoals bij doorgifte aan de leasemaatschappij. Bij verstrekking van uw gegevens aan onze verzuimverzekeraar hebben wij een gerechtvaardigd belang, namelijk dat wij daardoor aanspraak kunnen maken op een verzekeringsuitkering.

Daarnaast zijn er partijen die in onze opdracht werkzaamheden uitvoeren, zoals de accountant/boekhouder/salarisadministrateur. Bij deze

	doorgifte van uw gegevens hebben wij een gerechtvaardigd belang. Deze werkzaamheden zijn uitbesteed vanwege (onder meer) de kennis en expertise die onze accountant/boekhouder/salarisadministrateur bezit. Om de (arbeids)overeenkomst met u uit te voeren, heeft de accountant/boekhouder/salarisadministrateur uw persoonsgegevens nodig. *Verder maken wij gebruik van externe serverruimte voor de opslag van (delen van) onze personeels- en loonadministratie, waar uw persoonsgegevens onderdeel van uitmaken. Uw persoonsgegevens worden om die reden aan onze serverprovider verstrekt. Daarnaast maken wij gebruik van Microsoft Office en de bijbehorende opslagmogelijkheden voor e-mails en andere bestanden. Wij hebben bij deze twee doorgiften een gerechtvaardigd belang, omdat wij gegevens digitaal willen opslaan en verwerken en uitbesteding hiervan verschillende voordelen heeft.* ***Bewaarperiode persoonsgegevens*** *Wij zullen uw sollicitatiegegevens uiterlijk 4 weken na het eindigen van de sollicitatieprocedure verwijderen, tenzij u ons toestemming heeft gegeven om uw gegevens voor een periode van maximaal 1 jaar te bewaren.* *De persoonsgegevens uit de salarisadministratie die fiscaal van belang zijn zullen wij bewaren gedurende een periode van 7 jaar nadat u uit dienst bent getreden. Deze bewaartermijn hangt samen met een voor ons geldende wettelijke verplichting. Loonbelastingverklaringen en een kopie van uw identiteitsbewijs zullen wij 5 jaar na het einde van uw dienstverband bewaren. Ook deze bewaartermijn hangt samen met een voor ons geldende wettelijke verplichting.* *Voor andere gegevens uit de personeels- of loonadministratie hanteren wij een bewaartermijn van uiterlijk 2 jaar nadat uw dienstverband is beëindigd, tenzij blijkt dat bepaalde persoonsgegevens voor ons noodzakelijk zijn om te voldoen aan een wettelijke (bewaar)plicht of als sprake is van een arbeidsconflict of rechtszaak. Bij 'andere gegevens uit de personeels- of loonadministratie' moet u bijvoorbeeld denken aan arbeidsovereenkomsten, verslagen van beoordelings- en functioneringsgesprekken, correspondentie over benoeming, promotie, degradatie en ontslag, getuigschriften en administratieve verzuimgegevens.* ***Uw rechten*** *U heeft het recht om ons te vragen om uw eigen persoonsgegevens te mogen inzien. Als daartoe aanleiding bestaat, kunt u ons ook verzoeken om aanvulling van uw persoonsgegevens of om het wijzigen van onjuistheden. Daarnaast heeft u het recht om te vragen om uw persoonsgegevens te wissen of het gebruik van uw persoonsgegevens te beperken. Ook kunt u bij ons bezwaar maken tegen het verzamelen en gebruiken van uw gegevens. Vindt u dat wij onjuist omgaan met uw persoonsgegevens dan kunt u hierover een klacht indienen bij de organisatie die toezicht houdt op de privacyregels, de Autoriteit Persoonsgegevens. Tot slot kunt u ons verzoeken om verkrijging van uw persoonsgegevens of overdracht van die gegevens aan een ander.* *U kunt de hierboven genoemde rechten niet onder alle omstandigheden uitoefenen. Hebben wij uw persoonsgegevens bijvoorbeeld nodig om de wet na te leven, dan kunt u geen bezwaar maken of verzoeken om wissing.* *Om uw rechten te kunnen uitoefenen kunt u zich wenden tot: (**...uw bedrijfsnaam / specifieke contactpersoon van uw bedrijf, adres, postcode, plaats, telefoonnummer en e-mailadres...**). Ook met vragen of voor meer informatie over het verzamelen en gebruiken van uw persoonsgegevens kunt u uiteraard contact met ons opnemen.*	

§ 3.5 (deel 2)	Neem de privacyverklaring voor uw werknemers op in uw personeels-/bedrijfsreglement of personeelsgids of plaats de verklaring op een duidelijke en zichtbare plaats op het intranet/werknemersportaal. Heeft u geen bedrijfs- of personeelsreglement en intranet of werknemersportaal, dan zou u de privacyverklaring als bijlage aan de arbeidsovereenkomst kunnen hechten. De privacyverklaring moet u in ieder geval aan al uw werknemers verstrekken. Verwijs sollicitanten bij het eerste contact naar uw privacyverklaring en verstrek hen een exemplaar. Bij sollicitanten zal het eerste contactmoment veelal het toezenden van een ontvangstbevestiging op de sollicitatie zijn. U kunt hiervoor de volgende tekst gebruiken: *Wij maken u erop attent dat wij de persoonsgegevens die u ons heeft verstrekt en eventueel nog zult verstrekken, zullen verwerken op de manier zoals wij die in onze privacyverklaring hebben omschreven. Een kopie van onze privacyverklaring treft u in de bijlage aan.* Stuur daadwerkelijk een kopie van de privacyverklaring mee (bijvoegen als pdf bij de e-mail of een uitgeprint exemplaar bij uw brief).	
§ 3.7 (deel 2)	Als u beheer van (een deel van) uw personeels- of loonadministratie uitbesteedt aan een externe partij, persoonsgegevens opslaat op servers van een externe partij of wanneer de arbodienst of bedrijfsarts ook niet-medische persoonsgegevens verzamelt en gebruikt: sluit met deze partijen een "verwerkersovereenkomst" en gebruik hiervoor de overeenkomst uit bijlage 2. Ga na of de verwerkers voldoen aan de AVG.	
§ 2.3 (alg deel)	Houd een actueel overzicht bij van alle incidenten met persoonsgegevens die zich binnen uw bedrijf en bij uw verwerkers voordoen: noteer minimaal de feiten, omstandigheden, gevolgen en maatregelen omtrent deze incidenten. Maak voor de wijze van documenteren gebruik van de vragenlijst uit bijlage 3. Dit actiepunt hoeft u niet uit te voeren als u dit al had gedaan in het kader van de vorige checklist (klant- en leveranciersadministratie).	
§ 2.1 (alg deel)	Tref passende (organisatorische en technische) maatregelen ter beveiliging van de persoonsgegevens die onderdeel zijn van uw personeels- en loonadministratie. Bespreek met behulp van de informatie uit § 2.1 van het algemene deel met uw ICT 'er het huidige beveiligingsniveau per administratief onderdeel, of dit vanuit zijn vakgebied passend kan worden geacht en wat er aanvullend nog zou moeten gebeuren. Leg de uitkomsten vast in een document. Dit actiepunt hoeft u niet uit te voeren als u dit al had gedaan in het kader van de vorige checklist (klant- en leveranciersadministratie).	
Hfd. 7 (alg deel)	Vul voor de personeels- en loonadministratie het register in dat is opgenomen in bijlage 4. Dit register moet een overzicht bieden van alle verwerkingen die u uitvoert. Ook uw verwerkers moeten een register invullen voor de verwerkingen die zij onder uw verantwoordelijkheid uitvoeren. U kunt per administratief onderdeel een apart register invullen. Als het goed is, heeft u in het kader van de vorige checklist al een register voor uw klant- en leveranciersadministratie ingevuld. U moet ervoor zorgen dat het register een juiste weergave is en blijft van de verwerkingen die in de praktijk plaatsvinden. Daarom zult u het in de toekomst zo nodig moeten aanpassen.	
Hfd. 8 (alg deel)	Geef in de rechterkolom van deze actiepuntenlijst aan of u het punt heeft uitgevoerd en schrijf zo nodig in een bijlage bij het actiepunt meer in detail op hoe u in de praktijk uitvoering heeft gegeven aan het desbetreffende actiepunt. Documenteer eveneens waarom u vindt dat u iets niet hoeft te doen (bijv. waarom u géén FG hoeft aan te stellen). Als u verwerkingen binnen uw personeels- en loonadministratie baseert op de grondslag 'gerechtvaardigd belang', leg dan ook de afweging van de belangen schriftelijk vast.	

Bijlagen:

- […] *noemt u hier de eventuele bijlagen die horen bij het laatste actiepunt in de lijst hierboven.*

Hoofdstuk 3: Toelichting op de actiepuntenlijst

§ 3.1 Verwerking persoonsgegevens werknemers

Alle bedrijven die werknemers in dienst hebben, dus ook mkb'ers in de metaalbranche, verwerken persoonsgegevens van hun werknemers. Ook persoonsgegevens van sollicitanten en ex-werknemers worden hierdoor verwerkt. Daarnaast werken de meeste bedrijven (al dan niet incidenteel) ook met uitzendkrachten en stagiaires.

U bent als werkgever die personeel in dienst heeft wettelijk verplicht een personeelsadministratie te voeren. De verplichting om bij arbeidsrelaties bepaalde persoonsgegevens te verwerken vloeit vaak rechtstreeks voort uit arbeids- en belastingwetgeving. Sommige gegevens heeft u namelijk nodig om te kunnen voldoen aan wettelijke verplichtingen, zoals het betalen van belasting en premies. Andere gegevens zijn weer belangrijk voor het personeelsbeleid.

Werkgevers zijn dan ook verwerkers van persoonsgegevens en u bent verantwoordelijk voor de privacy van de werknemers. U en de eventueel door u ingeschakelde verwerkers (denk hierbij aan salaris- en/of administratiebedrijven) beschikken over een grote hoeveelheid privacygevoelige informatie. U was hierdoor al verplicht om:

- deze gegevens goed te beveiligen;
- de gegevens juist en nauwkeurig te registreren en niet langer dan noodzakelijk te bewaren;
- de werknemers de mogelijkheid te bieden de gegevens in te zien en indien nodig te corrigeren;
- de werknemers te informeren over het doel van de gegevensverzameling;
- slechts de noodzakelijke gegevens om de arbeidsovereenkomst uit te voeren vast te leggen in het personeelsdossier; en
- een bewerkersovereenkomst te sluiten met eventuele derde partijen die de personeelsgegevens bewerken.

De regelgeving geldt ook voor stagiaires of tijdelijk ingehuurde arbeidskrachten, omdat de privacy rechten van werknemers niet zijn beperkt tot werknemers met een vast contract. Alle natuurlijke personen die zich in een vergelijkbare positie bevinden als werknemers, genieten dezelfde bescherming.

Bij de gegevens die worden opgenomen in de personeelsadministratie kunt u (onder meer) denken aan:

a) personeelsgegevens rondom de persoon van de werknemer (NAW-gegevens);
b) kopie van het identiteitsbewijs;
c) gegevens omtrent het salaris en het bankrekeningnummer van de werknemer;
d) verslagen van beoordelings-, evaluatie- of functioneringsgesprekken, klachten en waarschuwingen;
e) telefoonabonnementen en leasecontracten; en
f) vaak ook (medische) gegevens in het kader van ziek- en herstelmeldingen.

Ondernemingsraden spelen een belangrijke rol bij de bescherming van de privacy van werknemers. Indien deze binnen uw bedrijf is ingesteld, heeft de ondernemingsraad bijvoorbeeld een instemmingsrecht bij regelingen voor het verwerken en beschermen van persoonsgegevens van werknemers. Dit instemmingsrecht geldt ook voor "voorzieningen die gericht zijn op waarneming of controle ten aanzien van aanwezigheid, gedrag of prestaties van werknemers". Voor bijvoorbeeld het opstellen en instellen van een internet- of e-mailprotocol of het invoeren van een personeelvolgsysteem is dus de instemming van de ondernemingsraad nodig. Voorbeelden van personeelvolgsystemen zijn: (verborgen) cameratoezicht, software voor de controle op e-mail- en internetgebruik en een prikklok of andere systemen van toegangscontrole.

Over een aantal onderwerpen moet u de ondernemingsraad om advies (in plaats van instemming) vragen. Een van die onderwerpen met een adviesrecht is de invoering of wijziging van een belangrijke technologische voorziening. Omdat gegevens tegenwoordig bijna alleen nog maar digitaal worden verwerkt, is dit een onderwerp dat ook vaak privacy gerelateerd is.

§ 3.2 Rechtmatigheid van de verwerkingen

Een goed personeelsdossier bevat alle actuele gegevens op basis waarvan u beslissingen over uw werknemers, zoals salarisverhoging of ontslag, kunt onderbouwen. Maar persoonsgegevens van werknemers mag u alleen verwerken voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. De verwerking moet dus telkens berusten op ten minste één van de zes wettelijke grondslagen (de rechtmatigheid van de verwerking), zie hiervoor paragraaf 1.2 van het algemene deel. U hanteert daarbij altijd het principe van "minimale gegevensverwerking", wat inhoudt dat u in beginsel alleen de voor de uitvoering van de (arbeids)overeenkomst noodzakelijke persoonsgegevens verwerkt. De gegevens mag u niet verwerken op een wijze die onverenigbaar is met de hiervoor bedoelde doeleinden.

Indien de verwerking bijvoorbeeld noodzakelijk is in verband met het sluiten of de uitvoering van een overeenkomst, kan aan het vereiste van een wettelijke grondslag zijn voldaan. In de relatie met de werknemer zal het gaan om de arbeidsovereenkomst die u met hem bent aangegaan. De oproepovereenkomst (ook wel het 0-urencontract genoemd) is vanzelfsprekend ook gewoon een arbeidsovereenkomst. Met de stagiair zult u een stageovereenkomst aangaan. Bij het werken met uitzendkrachten is sprake van een driehoeksverhouding tussen de uitzendkracht, het uitzendbureau (de uitlener) en u als opdrachtgever (inlener). Een uitzendkracht is over de periode dat hij voor u werkt, werkzaam op grond van een arbeidsovereenkomst die de uitzendkracht met het uitzendbureau sluit. Het uitzendbureau is dan ook de formele werkgever, hoewel de uitzendkracht feitelijk werkzaam is voor een derde, namelijk voor u als opdrachtgever/inlener. U zult daarom ook (via het uitzendbureau) de beschikking krijgen over persoonsgegevens van de uitzendkracht.

Naast de uitvoering van de (arbeids)overeenkomst kan ook de toestemming van de werknemer een wettelijke grondslag voor de verwerking vormen. Hoewel deze grondslag het eenvoudigst lijkt om te gebruiken en in het algemeen ook een van de belangrijkste en meeste gebruikte wettelijke grondslagen voor verwerking is, ligt dit in de specifieke relatie werkgever-werknemer anders. De werknemer heeft in deze relatie immers altijd een (financieel) afhankelijke positie, althans er is sprake van een gezagsverhouding ten opzichte van de werkgever. Hierdoor wordt er niet snel aangenomen dat de werknemer daadwerkelijk vrijelijk toestemming heeft gegeven. Het is daarom af te raden om werknemers bij indiensttreding al in zijn algemeenheid om toestemming te vragen voor de verwerking van persoonsgegevens, bijvoorbeeld door een dergelijk toestemmingsbeding op te nemen in de arbeidsovereenkomst. Dit algemene beding heeft geen enkele waarde, omdat het niet voldoet aan de specifieke eisen die aan de verwerkingsgrondslag toestemming worden gesteld.

Bijna alle werkgevers maken op enige manier gebruik van monitoring van werknemers. Hierbij kunt u denken aan het maken van camerabeelden, het controleren van e-mail, gebruikmaking van toegangspasjes en -systemen, assessments, tracking- en/of locatiegegevens van bedrijfsauto's of software die internetverkeer bijhoudt. Bij monitoring van werknemers moet u zich altijd afvragen:

1) of daarvoor een gerechtvaardigd belang aanwezig is;
2) hoe zwaar uw belangen wegen tegenover die van uw werknemers;
3) of de gekozen vorm van monitoring daarvoor noodzakelijk is;
4) of het doel wellicht op een minder ingrijpende manier kan worden bereikt; en
5) wat de ondernemingsraad vindt van de monitoring (denk aan het instemmings- of adviesrecht van de ondernemingsraad).

Een aantal verwerkingen moet, ondanks een eventueel gerechtvaardigd belang, altijd worden vermeden. In deze gevallen weegt de privacy en het belang van de werknemer in de regel zwaarder dan het belang van de werkgever:

- monitoring in gevoelige ruimten, zoals sanitaire-, religieuze- en pauzeruimten;
- het continu monitoren in plaats van steekproefsgewijs;
- camera's gebruiken voor de beoordeling van werknemers;
- geautomatiseerde beslissingen nemen over bijvoorbeeld prestaties;
- het maken van opnames met verborgen camera's. Dit mag alleen in zeer uitzonderlijke gevallen, zoals bij een gegronde verdenking van een strafbaar feit of het lekken van bedrijfsgeheimen.

Kortom, het is belangrijk om goed te beoordelen of een bepaalde verwerking rechtmatig is en om de grondslag van de verwerking indien mogelijk op een andere grondslag dan toestemming te baseren (bijvoorbeeld de noodzakelijkheid van de verwerking in het kader van de uitvoering van de

arbeidsovereenkomst). Zo kan een werkgever bijvoorbeeld salarisgegevens verwerken in het kader van de uitvoering van de arbeidsovereenkomst.

Enkele voorbeelden van verwerkingen:

- *Indien u binnen uw bedrijf gebruikt maakt van een **smoelenboek** (vaak toegankelijk via intranet of digitaal), waarin naast zakelijke gegevens ook foto's van werknemers worden weergegeven, vormt dit een verwerking van persoonsgegevens die niet strikt noodzakelijk is. De van de werknemers gevraagde foto's zijn niet nodig voor de uitvoering van de arbeidsovereenkomst. Gelet op wat wij hierboven aangaven over de toestemmingsgrond in de relatie werkgever-werknemer, zou strikt genomen geen toestemming mogen worden gevraagd aan de werknemers voor het gebruiken van hun (pas)foto in het smoelenboek. Als oplossing hiervoor zou u de keuze voor het aanleveren van een foto bij de werknemer kunnen laten liggen. U biedt dan alleen de mogelijkheid om een foto (en privégegevens) aan te leveren, welke vervolgens zullen worden opgenomen in het smoelenboek. Hierbij mag dus geen enkele vorm van 'dwang' worden uitgeoefend door de werkgever. Hier tegenover staat natuurlijk wel dat u al snel te maken krijgt met een incompleet smoelenboek, waardoor voor een groot deel het nut hiervan verdwijnt.*

- *Indien u gebruikmaakt van **cameratoezicht** op de werkplaats of in kantoorruimten, moet u voor elke camera die u ophangt bepalen wat hiervoor het gerechtvaardigde belang is. De inzet van een camera moet noodzakelijk zijn om de gestelde doelen te bereiken, mensen moeten worden geïnformeerd dat (en waar) er cameratoezicht is vóórdat zij worden gefilmd, de beelden moeten adequaat worden beveiligd én het moet duidelijk zijn hoe lang de beelden worden bewaard en wie de beelden kan/mag bekijken. Het beveiligen van bedrijfseigendommen kan een gerechtvaardigd belang zijn dat opweegt tegen de privacy van de werknemers. U moet echter altijd onderzoeken of er wellicht minder ingrijpende middelen mogelijk zijn. Hierbij kunt u bijvoorbeeld denken aan een bewegingssensor of het ophangen van camera's die niet op de werkplek van werknemers zijn gericht. In ieder geval mag de camera er niet hangen om werknemers te controleren op bijvoorbeeld prestaties en aanwezigheid of om te worden gebruikt voor een ander doel.*

- *Ook indien u gebruikmaakt van een **trackingsysteem** in het vervoersmiddel van de werknemer is de belangrijkste voorwaarde dat u hiervoor een gerechtvaardigd belang heeft en dat het plaatsen van een trackingsysteem hiervoor noodzakelijk is. Een gerechtvaardigd belang kan zijn het voertuig terugvinden na diefstal of het kunnen nagaan welke (dienst)auto zich het dichtst in de buurt van de klant bevindt, zodat deze auto naar de klant kan worden gestuurd. Het 'real-time' in kunnen zien van locatiegegevens zal meestal te veel inbreuk maken op de privacy van de werknemer die zich met het vervoersmiddel verplaatst. Bij het belang van het terug kunnen vinden van het voertuig na diefstal zou het minder ingrijpend zijn om de locatiegegevens pas beschikbaar te maken als het vervoersmiddel bijvoorbeeld als gestolen is opgegeven of als de ramen zijn ingeslagen.*

- *Het opslaan van **medische dossiers van werknemers in verzuimsystemen** is niet zomaar toegestaan. Als werkgever mag u namelijk geen gegevens over de aard en oorzaak van de ziekte van werknemers verwerken. Daarom mag een bedrijfsarts of arbodienst de medische dossiers van werknemers niet opslaan in een verzuimsysteem dat de werkgever zelf gebruikt en beheert. U mag de bedrijfsarts of arbodienst wel vragen de medische dossiers van uw zieke werknemers op te slaan in het verzuimsysteem dat u zelf ook gebruikt als dit systeem extern wordt beheerd. De bedrijfsarts of arbodienst moet in zo'n geval een verwerkersovereenkomst afsluiten met de beheerder van het verzuimsysteem. Daar moet onder meer in staan dat alleen de bedrijfsarts/arbodienst toegang krijgt tot de medische dossiers en dat deze zich bij toegang via internet met zogeheten "meerfactorauthenticatie" moet identificeren. U moet er verder voor zorgen dat de werknemers weten waar zij terecht kunnen als zij inzage willen in hun medisch dossier.*

In de AVG is verder bepaald dat de lidstaten in hun nationale recht of in collectieve overeenkomsten (CAO's) specifieke regels kunnen vaststellen voor de verwerking van persoonsgegevens van werknemers in het kader van de arbeidsverhouding. Het kan daarbij bijvoorbeeld gaan om de voorwaarden waaronder persoonsgegevens in de arbeidsverhouding op basis van de toestemming van de werknemer mogen worden verwerkt, voorwaarden voor de uitvoering van de arbeidsovereenkomst, voor het beheer, de planning en de organisatie van de arbeid, voor gelijkheid, diversi-

teit, gezondheid en veiligheid op het werk, voor de uitoefening en het genot van individuele of collectieve rechten en voordelen en voor de beëindiging van de arbeidsverhouding.

Deze eventuele nadere regels mogen afwijken van de AVG. Vooralsnog is echter duidelijk dat in Nederland géén gebruik zal worden gemaakt van deze afwijkingsmogelijkheid die het mogelijk maakt om ten aanzien van werknemers aanvullende nationale wetgeving op te stellen. Mochten er op dit punt alsnog afwijkende regels worden vastgesteld in Nederland, dan zullen wij dit deel van de serie AVG zo nodig aanpassen.

Terug naar de checklist

§ 3.3 Bijzondere persoonsgegevens

Anders dan in deel 1 van deze serie (klant- en leveranciersbeheer) verwerkt metaalbedrijf Jansen in het kader van de personeels- en loonadministratie ook bijzondere persoonsgegevens. Dit zijn persoonsgegevens die door hun aard bijzonder gevoelig zijn (zie ook de opsomming van bijzondere persoonsgegevens in het profiel van metaalbedrijf Jansen). Bijzondere persoonsgegevens verdienen specifieke bescherming, omdat de verwerking ervan grote risico's kan meebrengen voor de betrokkenen.

Een persoonsgegeven is niet alleen bijzonder indien het direct het betreffende 'bijzondere onderwerp' onthult, maar ook indien de gegevens indirect informatie bevatten. Een voorbeeld van een bijzonder persoonsgegeven is het lidmaatschap van een vakbond van een werknemer. Indien u ergens een lijstje heeft opgeslagen met daarin de namen van de werknemers die lid zijn van een vakbond (*wat niet is toegestaan!*), dan gaat het om directe informatie over het bijzondere persoonsgegeven. Het is echter zeer waarschijnlijk dat u op een andere, indirecte, manier over deze informatie beschikt. Op grond van artikel 39 van de CAO voor het Metaalbewerkingsbedrijf en artikel 9.8 van de CAO in de Metalektro hebben werknemers namelijk recht op (gedeeltelijke) teruggaaf van de vakbondscontributie of doorbetaling van het salaris bij het bijwonen van een studiedag georganiseerd door de vakbond. Als u de aanvraag hiervan van de werknemer opslaat of het bewijs van de contributiebetaling gebruikt voor de fiscale verrekening in de werkkostenregeling, gaat het om gegevens die indirect de informatie omtrent het lidmaatschap van de vakbond onthullen. Ook in dit laatste geval gaat het om bijzondere persoonsgegevens!

Volgens de huidige privacywet, de Wet bescherming persoonsgegevens, is het Burgerservicenummer (BSN) een bijzonder persoonsgegeven. Volgens de AVG is het BSN echter géén bijzonder persoonsgegeven, maar hier komen waarschijnlijk wel speciale regels voor. De lidstaten mogen onder de AVG namelijk zelf nadere voorwaarden stellen aan het verwerken van het BSN. Welke speciale regels hiervoor in Nederland gelden, staat op dit moment nog niet vast.

Kort gezegd is verwerking van bijzondere persoonsgegevens verboden, tenzij sprake is van een uitzondering genoemd in de AVG en dan alleen nog binnen de grenzen van die uitzondering.

Let op: In paragraaf 7.2 van het algemene deel is ingegaan op de uitzondering op de registratieplicht uit de AVG: ondernemingen of organisaties die minder dan 250 personen in dienst hebben hoeven geen register van verwerkingsactiviteiten bij te houden (registratieplicht). In drie gevallen kunt u echter géén beroep doen op deze uitzondering. Een van deze gevallen betreft het verwerken van bijzondere persoonsgegevens, wat metaalbedrijf Jansen in het kader van de personeels- en loonadministratie ook doet. Dit betekent dus dat ook voor werkgevers met een kleiner personeelsbestand de registratieplicht zal gelden. In hoofdstuk 7 van het algemene deel leest u wat de registratieplicht precies inhoudt en hoe u hieraan kunt voldoen.

§ 3.3.1 Welke bijzondere persoonsgegevens verwerkt metaalbedrijf Jansen?

Metaalbedrijf Jansen verwerkt natuurlijk niet alle soorten bijzondere persoonsgegevens. Wij gaan er hierbij vanuit dat zij niet verwerkt:

- persoonsgegevens waaruit politieke opvattingen blijken;
- persoonsgegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken;
- genetische gegevens; en
- gegevens over seksueel gedrag of seksuele gerichtheid.

Daarnaast gaan wij ervan uit dat metaalbedrijf Jansen geen persoonsgegevens verwerkt die betrekking hebben op strafrechtelijke feiten of veroordelingen.

Metaalbedrijf Jansen verwerkt (mogelijk) wel:

a. persoonsgegevens waaruit ras of etnische afkomst blijkt;
b. persoonsgegevens waaruit het lidmaatschap van een vakbond blijkt;
c. biometrische gegevens; en
d. gezondheidsgegevens.

a. Een voorbeeld van persoonsgegevens waaruit ras of etnische afkomst blijkt zijn de identiteitspasjes met foto's die de werkgever aan zijn werknemers verstrekt. Omdat een kopie van zulke pasjes in de regel door de werkgever wordt bewaard en opgeslagen, is doorgaans sprake van een verwerking van persoonsgegevens. Aangezien van de foto op het pasje het ras van de werknemer kan worden afgeleid, gaat het bovendien om een verwerking van een bijzonder persoonsgegeven. Een dergelijk pasje kan verstrekt worden met het oog op de identificatie van de werknemer bij het betreden van het gebouw van de werkgever. Het belang van de werkgever kan met zich brengen dat invoering van een pasjessysteem noodzakelijk is. Dit zal zich bijvoorbeeld kunnen voordoen bij grote werkgevers die veel werknemers in dienst hebben en waarbij identificatie bij het betreden van het terrein van de werkgever alleen op een juiste manier kan plaatsvinden aan de hand van een van een foto voorzien identiteitsbewijs.

b. Bij het lidmaatschap van een vakbond moet u niet alleen denken aan de bekende vakbonden (FNV, CNV, etc.), maar ook een personeelsvereniging kan hieronder vallen indien zij (mede) bij de werkgever opkomt voor werknemersbelangen. Indien deze vereniging zich echter alleen bezighoudt met organisatie van gezamenlijke activiteiten en zich verder dus niet richt op belangenbehartiging van de werknemers, dan is dit geen vakbond.

c. Bij biometrische gegevens kunt u denken aan portretten, een irisscan, vingerafdrukken of stemgeluid. Deze gegevens maken eenduidige identificatie mogelijk, omdat het gaat om unieke lichaamskenmerken die zijn te herleiden naar één individu. Vaak bevatten biometrische gegevens meer informatie dan strikt noodzakelijk zou zijn voor identificatie van de persoon. Biometrische gegevens zijn echter alleen bijzondere persoonsgegevens als ze worden verwerkt met het oog op identificatie. Bij een opname van een beveiligingscamera hangt dit dus van het doel van de opname af.

   - ***Foto's*** *kunnen onder bepaalde omstandigheden worden aangemerkt als biometrische gegevens. Dit is bijvoorbeeld het geval indien de foto's worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie van een natuurlijke persoon mogelijk maken.*

d. Gezondheidsgegevens omvatten alle persoonsgegevens over de fysieke of mentale gezondheid van een persoon, zowel in het heden, verleden als de toekomst. Het gaat om gegevens omtrent ziekte, handicap, ziekterisico, medische voorgeschiedenis, klinische behandeling of de fysiologische of biomedische staat van de betrokkene, ongeacht de bron waaruit deze informatie verkregen wordt. Ook uitslagen van onderzoeken aan het lichaam of aan lichaamseigen stoffen (zoals bloed) vallen onder gezondheidsgegevens.

Terug naar de checklist

§ 3.3.2 Uitzonderingen op het verbod

Zoals eerder aangegeven is de verwerking van bijzondere persoonsgegevens verboden, tenzij sprake is van een uitzonderingsgrond. De AVG formuleert voor de verwerking van bijzondere persoonsgegevens aparte uitzonderingsgronden, die dus anders zijn dan de grondslagen zoals genoemd in paragraaf 1.2 van het algemene deel.

De belangrijkste uitzonderingen voor het mogen verwerken van bijzondere persoonsgegevens zijn de volgende:

1) De uitdrukkelijke toestemming van de betrokkene voor de verwerking van die persoonsgegevens voor duidelijk omschreven doeleinden. Er moet sprake zijn van een expliciete wilsuiting gericht op het geven van toestemming. Uit een enkele handeling kan in beginsel geen toestemming worden afgeleid, tenzij die handeling 'ondubbelzinnig en actief is'. Zie in dit verband ook paragraaf 3.2 hierboven inzake het probleem met de toestemmingsgrond in de relatie werkgever-werknemer.

2) De verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van de verwerkingsverantwoordelijke of de betrokkene op het gebied van het arbeidsrecht en het socialezekerheids- en socialebeschermingsrecht. Dit moet in een wettelijke regeling of in een CAO zijn vastgelegd.

- *Voorbeeld: het lidmaatschap van uw werknemers van een vakbond mag u niet registreren in de (personeels)administratie. Wél mag u de benodigde gegevens gebruiken voor de uitvoering van een recht van de werknemer op grond van de CAO. Het gegeven dat een werknemer lid is van een vakbond kan hierdoor terugkomen in bijvoorbeeld de loonadministratie. Die verwerking was immers noodzakelijk voor de uitvoering van het specifieke recht van uw werknemer.*

3) De verwerking heeft betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt. Er mag daarbij geen twijfel zijn dat de persoon *zelf* gehandeld heeft om het persoonsgegeven openbaar te maken.

4) De verwerking is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering in het kader van gerechtelijke procedures. Een voorbeeld hiervan is het overleggen van een bewijsstuk aan de rechtbank.

5) De verwerking is noodzakelijk voor doeleinden van preventieve geneeskunde of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg, sociale diensten of behandelingen, etc.

Het verbod op verwerking geldt volgens de laatstgenoemde uitzondering dus niet indien dit noodzakelijk is voor medische redenen, met name in verband met de arbeid. Een voorbeeld hiervan is het beoordelen van de arbeids(on)geschiktheid van de werknemer. De medische handelingen moeten wel zijn vastgelegd in een wettelijke regeling of voorvloeien uit een medische behandelovereenkomst. Bovendien mogen deze gegevens, als dat noodzakelijk is voor de genoemde medische doeleinden, alleen worden verwerkt door een beroepsbeoefenaar die aan een wettelijk beroepsgeheim is gebonden. Dit zijn bijvoorbeeld artsen en advocaten. Andere personen of instellingen mogen dit dus niet, tenzij natuurlijk sprake is van een andere geldige uitzondering op het verbod.

De werkgever mag alleen gegevens inzien die noodzakelijk zijn voor het begeleiden van het verzuim, zoals een telefoonnummer/verpleegadres waarop de werknemer bereikbaar is, de verzuimduur en lopende afspraken.

Terug naar de checklist

§ 3.3.3 Andere uitzonderingsmogelijkheden

De AVG biedt op een aantal punten ruimte voor landen om zelf de regels nader te bepalen. Dat geldt bijvoorbeeld voor een aantal uitzonderingen op het verwerkingsverbod van bijzondere persoonsgegevens, zoals hierboven genoemd. Nederland legt de invulling van deze uitzonderingen voornamelijk vast in de zogeheten 'Uitvoeringswet AVG'. Hoewel deze wet op dit moment nog niet definitief is vastgesteld, zijn de nadere regels nodig voor de uitvoering van de AVG en daarom zal de wet ook op 25 mei 2018 (gelijktijdig met de AVG) in werking treden.

De technische mogelijkheden om met behulp van biometrische kenmerken van een persoon iemand te identificeren zijn sterk in ontwikkeling. Veel bedrijven werken daarnaast al met biometrische toegangscontrole voor locaties. Daarom heeft Nederland in de Uitvoeringswet AVG voorzien in een extra uitzonderingsmogelijkheid ten aanzien van het verwerken van **biometrische gegevens**:

"*Het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken is niet van toepassing, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden*."

Het blijft hierbij noodzakelijk om een juiste belangenafweging te maken, maar binnen deze kaders komt er in Nederland dus wél ruimte voor het gebruik van biometrie. De werkgever zal telkens moeten afwegen of de gebouwen of systemen zodanig beveiligd moeten zijn dat dit met biometrie moet gebeuren. Het verwerken van biometrische gegevens moet daarnaast ook proportioneel zijn. Als het om de toegang tot een garage van een reparatiebedrijf gaat, zal de noodzaak van de beveiliging niet zodanig zijn dat werknemers alleen met biometrie toegang kunnen krijgen. Zonder deze specifieke uitzondering in de Uitvoeringswet is er in de relatie tussen werkgever en werknemer eigenlijk geen andere bruikbare uitzondering voor het rechtmatig gebruikmaken van biometrie door de werkgever. Zo kan de uitzondering van uitdrukkelijke toestemming juist in de relatie werkgever-werknemer vrijwel niet worden gebruikt.

Verder voorziet de Uitvoeringswet in een artikel dat een uitzondering maakt op het verbod om persoonsgegevens te verwerken waaruit **ras of etnische afkomst** blijkt:

"Het verbod om persoonsgegevens te verwerken waaruit ras of etnische afkomst blijkt, is niet van toepassing, indien de verwerking geschiedt met het oog op de identificatie van de betrokkene, en slechts voor zover de verwerking voor dat doel onvermijdelijk is".

De Uitvoeringswet voert ook een artikel in voor verwerkingen van **gezondheidsgegevens**. In het artikel zijn de uitzonderingen op het verbod om medische gegevens te verwerken opgenomen, die in sommige gevallen ook voor werkgevers gelden.

Kort gezegd is bepaald dat het verbod om gegevens over gezondheid te verwerken niet van toepassing is als de verwerking geschiedt door werkgevers voor zover dat noodzakelijk is voor een goede uitvoering van de wet of de CAO. De wet of de CAO moet daarbij wel voorzien in bepaalde rechten van de werknemer die afhankelijk zijn van zijn gezondheidstoestand. Zo bent u als werkgever op grond van de wet en de CAO voor het Metaalbewerkingsbedrijf verplicht om zieke werknemers twee jaar lang loon door te betalen. U mag dan gegevens over de gezondheid van zieke werknemers verwerken voor zover die noodzakelijk zijn om het recht op loondoorbetaling vast te stellen. Indien een werknemer zich ziek meldt, hoeft hij u dus niet ook de aard en de oorzaak van de ziekte mede te delen, want dat is niet noodzakelijk voor de vaststelling van het recht op loondoorbetaling.

Het verbod om gegevens over gezondheid te verwerken is ook niet van toepassing als de verwerking geschiedt door werkgevers en noodzakelijk is voor de re-integratie of begeleiding van werknemers. Gegevens over de medische achtergronden van de arbeidsongeschiktheid mogen niet door u worden verwerkt. U mag alleen gegevens verwerken omtrent het feit dat en de mate waarin de werknemer arbeidsongeschikt is, alsmede de periode van arbeidsongeschiktheid.

Terug naar de checklist

§ 3.4 Informatie die u moet verstrekken

Hieronder zullen wij de informatie opsommen die u in zijn algemeenheid aan uw werknemers moet verstrekken. Daarbij zullen wij uiteraard aangeven hoe bij het onderdeel 'personeels- en loonadministratie' concreet invulling kan worden gegeven aan de informatieplicht. In de volgende paragraaf zullen wij aangeven op welke wijze u de informatie aan de werknemers kunt verstrekken. Zo mogelijk doen wij ook concrete tekstvoorstellen, die ook zijn opgenomen in de actiepuntenlijst voorin dit deel van de serie.

Indien de werknemers formeel in dienst zijn van een andere vennootschap, bijvoorbeeld bij een aparte personeels-B.V. binnen het concern, dan geldt het onderstaande voor deze personeels-B.V.

Te verstrekken informatie:

1. U moet de werknemers informeren over uw identiteit en uw contactgegevens.

Wij raden minimaal aan de volgende gegevens te verstrekken: uw naam (incl. rechtsvorm), vestigingsadres, postcode, plaats, telefoonnummer en e-mailadres.

2. Als u een functionaris voor gegevensbescherming heeft, dan moet u de contactgegevens van deze persoon verstrekken.

   De meeste Metaalunieleden hoeven geen functionaris aan te stellen (zie hoofdstuk 4 van het algemene deel). Deze informatieverplichting komt daardoor voor hen te vervallen.

3. U moet de werknemers vertellen waarom u hun persoonsgegevens wilt verwerken. Met andere woorden: wat is uw doel? Ook moet u aangeven welke grondslag u hiervoor gebruikt. Als sprake is van de grondslag 'gerechtvaardigd belang', moet dit belang worden benoemd en gemotiveerd. Verder moet u aangegeven of verstrekking van persoonsgegevens noodzakelijk is voor een wettelijke of contractuele plicht of een noodzakelijke voorwaarde is om de (arbeids)overeenkomst aan te gaan, of de werknemer verplicht is persoonsgegevens te verstrekken en wat de gevolgen zijn als hij dat niet doet.

   U zou aan deze informatieverplichting kunnen voldoen door middel van onderstaande tekst:

   Verzamelen en gebruiken van persoonsgegevens van sollicitanten, uitzendkrachten/payroll-werknemers, stagiaires en werknemers
   Graag maken wij u er op attent dat wij de persoonsgegevens die u ons verstrekt zullen verzamelen en gebruiken omdat dit noodzakelijk is voor het doorlopen van de sollicitatieprocedure of om een (eventuele) arbeidsovereenkomst / stageovereenkomst / uitzendovereenkomst te sluiten en uit te voeren. Daarnaast zijn bepaalde persoonsgegevens nodig voor de nakoming en uitvoering van bepalingen uit de voor ons geldende CAO. Ook verzamelen en gebruiken wij uw persoonsgegevens om aan bepaalde wettelijke verplichtingen te kunnen voldoen. Deze wettelijke verplichtingen hebben bijvoorbeeld te maken met de vaststelling en verschuldigdheid van belastingen en premies voor werknemers.

   Gelet op deze noodzaak bent u verplicht om de hiervoor benodigde persoonsgegevens aan ons te verstrekken. Als u ons geen of onvoldoende persoonsgegevens verstrekt, dan kunnen wij mogelijk geen sollicitatieprocedure met u doorlopen, een (eventuele) arbeidsovereenkomst / stageovereenkomst / uitzendovereenkomst met u aangaan en uitvoeren of aan onze wettelijke verplichtingen voldoen.

   Bent u (payroll-)werknemer of stagiair, dan gebruiken wij uw gegevens voor het opstellen, uitvoeren en beëindigen van de arbeids- of stageovereenkomst of de arbeidsrelatie. Hieronder wordt onder meer verstaan:
   a) de behandeling van personeelszaken;
   b) het vaststellen en uitbetalen van het salaris, vergoedingen en andere geldbedragen; en
   c) het vaststellen en betalen van eventuele belastingen, premies en andere fiscale verplichtingen ten behoeve van u als werknemer of stagiair.

   Bent u een sollicitant, dan gebruiken wij uw gegevens om met u te kunnen communiceren over het verloop van de sollicitatieprocedure, de beoordeling van uw geschiktheid voor een functie die vacant is of kan komen en de eventuele afhandeling van de door u gemaakte onkosten.

   Bent u een uitzendkracht, dan zullen wij de gegevens die wij verkrijgen van het uitzendbureau gebruiken voor de beoordeling van uw geschiktheid voor een functie die vacant is of kan komen en voor de uitvoering van de uitzendovereenkomst.

4. Als u persoonsgegevens aan andere partijen/derden doorgeeft, dan moet u de werknemers informeren over de ontvangers of categorieën van ontvangers.

   In het kader van de arbeidsrelatie met uw werknemers zullen in bijna alle gevallen ook andere organisaties persoonsgegevens van de werknemers verwerken. Denk hierbij bijvoorbeeld aan de externe personeelsdienst, boekhouder/accountant, arbodienst, verzuimverzekeraar, het pensioenfonds en de leasemaatschappij. Ook bij gebruikmaking van server-/opslagruimte bij

een derde worden vaak persoonsgegevens doorgegeven. Aan uw informatieverplichting hierover kunt u voldoen door gebruik te maken van onderstaande tekst:

Doorgifte aan derden
*Het is mogelijk dat wij uw persoonsgegevens doorgeven aan andere partijen. Deze andere partijen kunnen overheidsorganen zijn, maar ook partijen die in onze opdracht werkzaamheden uitvoeren of partijen aan wie wij verplicht zijn gegevens te verstrekken in verband met de (uitvoering van de) arbeidsovereenkomst. Het gaat om de volgende partijen: [**graag verder aanvullen of aanpassen**]*

- *de Belastingdienst;*
- *het UWV;*
- *onze arbodienst/bedrijfsarts;*
- *de Inspectie voor Sociale Zaken en Werkgelegenheid;*
- *het Pensioenfonds;*
- *de leasemaatschappij;*
- *de verzuimverzekeraar;*
- *onze accountant/boekhouder/salarisadministrateur;*
- *[…]*
- *[…]*

Soms zal het verstrekken van uw gegevens aan een ander noodzakelijk zijn om te kunnen voldoen aan de wet, zoals het geval is bij doorgifte aan de Belastingdienst, het UWV, de arbodienst/bedrijfsarts, het (verplicht gestelde) Pensioenfonds en de Inspectie voor Sociale Zaken en Werkgelegenheid.

In andere gevallen is de doorgifte noodzakelijk om de (arbeids)overeenkomst met u te kunnen uitvoeren, zoals bij doorgifte aan de leasemaatschappij. Bij verstrekking van uw gegevens aan onze verzuimverzekeraar hebben wij een gerechtvaardigd belang, namelijk dat wij daardoor aanspraak kunnen maken op een verzekeringsuitkering.

Daarnaast zijn er partijen die in onze opdracht werkzaamheden uitvoeren, zoals de accountant/boekhouder/salarisadministrateur. Bij deze doorgifte van uw gegevens hebben wij een gerechtvaardigd belang. Deze werkzaamheden zijn uitbesteed vanwege (onder meer) de kennis en expertise die onze accountant/boekhouder/salarisadministrateur bezit. Om de (arbeids)overeenkomst met u uit te voeren, heeft de accountant/boekhouder/salarisadministrateur uw persoonsgegevens nodig.

Verder maken wij gebruik van externe serverruimte voor de opslag van (delen van) onze personeels- en loonadministratie, waar uw persoonsgegevens onderdeel van uitmaken. Uw persoonsgegevens worden om die reden aan onze serverprovider verstrekt. Daarnaast maken wij gebruik van Microsoft Office en de bijbehorende opslagmogelijkheden voor e-mails en andere bestanden. Wij hebben bij deze twee doorgiften een gerechtvaardigd belang, omdat wij gegevens digitaal willen opslaan en verwerken en uitbesteding hiervan verschillende voordelen heeft.

5. Als u persoonsgegevens aan partijen/derden doorgeeft die buiten de EER zijn gevestigd, dan bent u verplicht om de werknemers te laten weten of dit land adequaat is verklaard door de Europese Commissie. Is zo'n besluit er niet, dan moet u aangeven welke passende en geschikte waarborgen dit land dan biedt ter bescherming van persoonsgegevens, hoe hier een kopie van kan worden verkregen of waar deze kunnen worden geraadpleegd.

   Meestal is deze situatie niet van toepassing. Wel kan hiervan sprake zijn als bijvoorbeeld een kopie van bepaalde personeelsgegevens van werknemers centraal wordt opgeslagen op een server van het hoofdkantoor in het buitenland. Voor een verdere toelichting op doorgifte van persoonsgegevens aan derden verwijzen wij u graag naar hoofdstuk 6 van het algemene deel.

6. U moet de werknemers informeren over hoe lang u hun persoonsgegevens gaat bewaren.

   De verschillende (wettelijke) bewaartermijnen veranderen niet onder de AVG. De specifieke bewaartermijn in het kader van de personeelsadministratie hangt af van het soort gegevens.

   - Voor gegevens uit de salarisadministratie die fiscaal van belang zijn geldt een bewaartermijn van 7 jaar nadat de werknemer uit dienst is.

- Voor de loonbelastingverklaring en een kopie van het identiteitsbewijs geldt een bewaartermijn van 5 jaar na het einde van het dienstverband.
- Bij sollicitatiegegevens is het gebruikelijk om de sollicitatiegegevens te verwijderen uiterlijk 4 weken na het einde van de sollicitatieprocedure, tenzij de sollicitant toestemming heeft gegeven om de gegevens langer te bewaren (een termijn van maximaal 1 jaar is hiervoor redelijk).
- Geen wettelijke bewaartermijnen gelden voor andere categorieën gegevens zoals verslagen van beoordelings- en functioneringsgesprekken, arbeidsovereenkomsten, correspondentie over benoeming, promotie, degradatie en ontslag, getuigschriften en administratieve verzuimgegevens. Voor dit soort gegevens is de richtlijn: een bewaartermijn uiterlijk 2 jaar nadat het dienstverband of de werkzaamheden van de betrokkene zijn beëindigd, tenzij de persoonsgegevens noodzakelijk zijn ter voldoening aan een wettelijke bewaarplicht. Als de gegevens al eerder niet meer nodig zijn, moet u ze vanaf dat moment verwijderen.

Indien tussen de werkgever en de werknemer een arbeidsconflict bestaat of er een rechtszaak loopt, kan de werkgever de gegevens van de (ex-)werknemer langer bewaren.

De tekst die u voor uw informatieverplichting over de bewaartermijnen kunt gebruiken luidt als volgt:

> ***Bewaarperiode persoonsgegevens***
> *Wij zullen uw sollicitatiegegevens uiterlijk 4 weken na het eindigen van de sollicitatieprocedure verwijderen, tenzij u ons toestemming heeft gegeven om uw gegevens voor een periode van maximaal 1 jaar te bewaren.*
>
> *De persoonsgegevens uit de salarisadministratie die fiscaal van belang zijn zullen wij bewaren gedurende een periode van 7 jaar nadat u uit dienst bent getreden. Deze bewaartermijn hangt samen met een voor ons geldende wettelijke verplichting. Loonbelastingverklaringen en een kopie van uw identiteitsbewijs zullen wij 5 jaar na het einde van uw dienstverband bewaren. Ook deze bewaartermijn hangt samen met een voor ons geldende wettelijke verplichting.*
>
> *Voor andere gegevens uit de personeels- of loonadministratie hanteren wij een bewaartermijn van uiterlijk 2 jaar nadat uw dienstverband is beëindigd, tenzij blijkt dat bepaalde persoonsgegevens voor ons noodzakelijk zijn om te voldoen aan een wettelijke (bewaar)plicht of als sprake is van een arbeidsconflict of rechtszaak. Bij 'andere gegevens uit de personeels- of loonadministratie' moet u bijvoorbeeld denken aan arbeidsovereenkomsten, verslagen van beoordelings- en functioneringsgesprekken, correspondentie over benoeming, promotie, degradatie en ontslag, getuigschriften en administratieve verzuimgegevens.*

7. U moet de werknemers wijzen op de rechten die zij hebben. Het gaat dan om het recht op inzage, rectificatie, wissing, beperking van verwerking, bezwaar, digitale overdracht van de persoonsgegevens en het recht om een klacht in te dienen bij de AP. Hieronder doen wij een tekstvoorstel voor deze verplichting:

> ***Uw rechten***
> *U heeft het recht om ons te vragen om uw eigen persoonsgegevens te mogen inzien. Als daartoe aanleiding bestaat, kunt u ons ook verzoeken om aanvulling van uw persoonsgegevens of om het wijzigen van onjuistheden. Daarnaast heeft u het recht om te vragen om uw persoonsgegevens te wissen of het gebruik van uw persoonsgegevens te beperken. Ook kunt u bij ons bezwaar maken tegen het verzamelen en gebruiken van uw gegevens. Vindt u dat wij onjuist omgaan met uw persoonsgegevens dan kunt u hierover een klacht indienen bij de organisatie die toezicht houdt op de privacyregels, de Autoriteit Persoonsgegevens. Tot slot kunt u ons verzoeken om verkrijging van uw persoonsgegevens of overdracht van die gegevens aan een ander.*
>
> *U kunt de hierboven genoemde rechten niet onder alle omstandigheden uitoefenen. Hebben wij uw persoonsgegevens bijvoorbeeld nodig om de wet na te leven, dan kunt u geen bezwaar maken of verzoeken om wissing.*
>
> *Om uw rechten te kunnen uitoefenen kunt u zich wenden tot: (**naam, adres, postcode, plaats, telefoonnummer en e-mailadres**). Ook met vragen of voor meer informatie over*

het verzamelen en gebruiken van uw persoonsgegevens kunt u uiteraard contact met ons opnemen.

8. U moet de werknemers laten weten dat zij de gegeven toestemming voor verwerking van hun persoonsgegevens ook weer mogen intrekken.

   In de arbeidsrelatie met de werknemer zal dit echter niet (snel) van toepassing zijn, omdat de toestemmingsgrond in de regel niet kan gelden in de relatie werkgever-werknemer (zie ook paragraaf 3.2 van dit deel van de serie).

9. U moet de werknemers vertellen of er op basis van zijn persoonsgegevens geautomatiseerde individuele besluiten worden genomen. Dit zijn besluiten die de uitkomst zijn van een computeranalyse (dus zonder menselijke tussenkomst genomen) en voor de betrokkene (rechts)gevolgen hebben.

   Bij de personeels- en loonadministratie zal van 'geautomatiseerde individuele besluiten' in de regel geen sprake zijn.

Wij adviseren om met ingang van 25 mei 2018 alle (nieuwe) werknemers, stagiaires, sollicitanten en uitzendkrachten/payroll-werknemers te informeren in overeenstemming met de bepalingen uit de AVG. De informatieplicht bestaat overigens onder de Wbp ook al, maar wordt in de AVG uitgebreid en gedetailleerder.

Terug naar de checklist

§ 3.5 De wijze en het moment waarop de informatie moet worden verstrekt

U moet de informatie uit de vorige paragraaf aan de werknemers verstrekken "bij de verkrijging van persoonsgegevens", aldus de AVG. U zult echter niet altijd kunnen informeren voorafgaand aan de verkrijging van persoonsgegevens: sollicitanten zullen u immers ook zelfstandig benaderen en daarbij meteen al persoonsgegevens verstrekken. Logischerwijs kunt u de sollicitant dan pas informeren in uw reactie op de brief/e-mail die deze potentiële werknemer u heeft gestuurd.

Wij adviseren u aan uw informatieverplichtingen te voldoen door de informatie die u moet geven op te nemen in een zogenaamde "privacyverklaring". De privacyverklaring moet u vervolgens aan al uw (potentiële) werknemers verstrekken. Indien u een bedrijfs- of personeelsreglement hebt, kunt u hierin een hoofdstuk "Privacy" opnemen waar de vereiste informatie wordt gegeven. Daarnaast kan de privacyverklaring worden opgenomen op intranet of het werknemersportaal. Plaats uw privacyverklaring (of het personeelsreglement met daarin opgenomen het privacy hoofdstuk) in ieder geval op een duidelijke en zichtbare plaats op het intranet of het werknemersportaal. Heeft u geen bedrijfs- of personeelsreglement en intranet of werknemersportaal, dan zou u de privacyverklaring als bijlage aan de arbeidsovereenkomst kunnen hechten.

Let er bovendien op dat de privacyverklaring telkens getoetst wordt aan nieuwe ontwikkelingen, dat de werknemers op de hoogte worden gesteld van aanpassingen en dat de verklaring consequent wordt verstrekt aan (nieuwe) werknemers.

U zult bij het eerste contact met een sollicitant het onderwerp privacy al ter sprake moeten brengen. Dat kan bijvoorbeeld al zijn bij het bekend maken van een vacature op uw website. Heeft u alleen schriftelijk of elektronisch contact met een sollicitant naar aanleiding van een open sollicitatie, dan zal dit eerste contact vaak bestaan uit het verzenden van een ontvangstbevestiging van de sollicitatiebrief. Gebruikt u de gegevens van de sollicitant in eerste instantie alleen voor het doorlopen van de sollicitatieprocedure, dan kunt u de volgende alinea opnemen in uw (ontvangst)bericht aan de sollicitant:

> *Wij maken u erop attent dat wij de persoonsgegevens die u ons heeft verstrekt en eventueel nog zult verstrekken, zullen verwerken op de manier zoals wij die in onze privacyverklaring hebben omschreven. Een kopie van onze privacyverklaring treft u in de bijlage aan.*

Voeg bij uw ontvangstbericht ook daadwerkelijk een exemplaar van uw privacyverklaring en vermeld het document onder een kopje "Bijlage(n)". Bij communicatie per e-mail kunt u de privacyverklaring als pdf bijvoegen.

De mededeling dat u een kopie meestuurt van uw privacyverklaring plaatst u bij voorkeur niet in de voettekst van een A4'tje. Doet u dat wel, dan is het daarmee een 'standaardtekst' geworden, en de mededeling dat een kopie is bijgevoegd verliest daardoor mogelijk zijn waarde.

In bijlage 1 treft u een privacyverklaring voor de personeels- en loonadministratie aan. In deze verklaring is dus alle informatie opgenomen waarover u uw werknemers moet informeren als u voldoet aan het profiel van metaalbedrijf Jansen.

Terug naar de checklist

§ 3.6 Toestemming vragen

In paragraaf 3.2 van dit deel gingen wij al in op 'het probleem' met de toestemmingsgrond in de relatie werkgever-werknemer. Dit heeft te maken met de ongelijke of afhankelijke verhouding tussen de werkgever en de werknemer. De werknemer kan zich al snel onder druk gezet voelen om toch zijn toestemming te geven, omdat hij onder gezag van de werkgever staat. Het kan echter voorkomen dat u niet kunt aantonen dat een (door u gewenste) verwerking van persoonsgegevens noodzakelijk is in verband met de uitvoering van de arbeidsovereenkomst of om een wettelijke verplichting uit te voeren. Denk hierbij bijvoorbeeld aan het bekend maken van de naam en directe contactgegevens of foto's van werknemers op uw website. Deze verwerking heeft niets te maken met het aangaan of uitvoeren van de arbeidsovereenkomst en is ook geen wettelijke verplichting.

Als u toch (andere dan de voor de uitvoering van de arbeidsovereenkomst noodzakelijke) persoonsgegevens gaat verwerken en u heeft daarvoor toestemming nodig van de werknemers, dan bepaalt de wet hierover het volgende.

De toestemming moet door middel van een verklaring of een andere ondubbelzinnige actieve handeling door de werknemer worden gegeven. De werknemer kan nooit stilzwijgend of op een passieve manier toestemming verlenen. Een actief handelen van zijn kant is dus noodzakelijk.

De toestemming geldt alleen als deze gebaseerd is op informatie van u over wat u met de gegevens gaat doen in duidelijke en eenvoudige taal. De informatie moet gemakkelijk toegankelijk zijn. De werknemer moet precies weten waar zijn toestemming op gericht zal zijn en uw informatie hierover moet duidelijk te onderscheiden zijn van andere aangelegenheden waarover u hem eventueel tegelijkertijd informeert. De werknemer mag op ieder moment zijn toestemming weer intrekken (en daar moet u hem ook over informeren).

Het heeft gelet op het voorgaande dan ook geen zin om werknemers bij het aangaan van de arbeidsovereenkomst in zijn algemeenheid om toestemming te vragen voor het verwerken van persoonsgegevens. Ook kunt u niet volstaan met een bepaling in de arbeidsovereenkomst dat het ondertekenen van de arbeidsovereenkomst impliceert dat de werknemer toestemming geeft voor verwerking van zijn persoonsgegevens. Aan het vereiste van 'ondubbelzinnigheid' is dan immers niet voldaan. Het instemmen met de arbeidsvoorwaarden uit de overeenkomst hoeft immers niet te betekenen dat de betrokkene ook toestemt met allerlei soorten (niet noodzakelijke) verwerkingen van zijn persoonsgegevens.

§ 3.7 Verwerkingsactiviteiten uitbesteden

In het profiel van metaalbedrijf Jansen hebben wij aangegeven dat metaalbedrijf Jansen de personeelsadministratie in eigen beheer heeft. Metaalbedrijf Jansen besteedt de loonadministratie wel (volledig of gedeeltelijk) uit aan een derde, namelijk haar externe loonadministrateur, boekhouder of accountant. Daarnaast werkt metaalbedrijf Jansen samen met de arbodienst, het pensioenfonds, de verzuimverzekeraar en leasemaatschappij.

Indien u de personeels- of loonadministratie uitbesteedt aan een derde blijft u verantwoordelijk voor de verwerkingen. De partij die de verwerkingsactiviteiten voor u uitvoert, wordt 'verwerker' genoemd. Hieronder wordt niet verstaan een partij aan wie u een opdracht tot het leveren van za-

ken of diensten uitbesteedt die niet zien op verwerking van persoonsgegevens. Als u een ander bedrijf opdracht geeft tot het vervaardigen van visitekaartjes voor uw werknemers dan is geen sprake van een verwerker, ook al gaat de derde hierbij persoonsgegevens verwerken. De opdracht ziet immers niet zozeer op verwerking van persoonsgegevens, maar op het leveren van zaken. Het verwerken van persoonsgegevens vloeit hier uit voort. Omdat dit voortvloeit uit de opdracht, heeft de opdrachtnemer ook geen zeggenschap over de verwerking (m.a.w. hij bepaalt niet welke gegevens worden verwerkt en hoe). Wanneer u een ander bedrijf vraagt om de loonadministratie te beheren, dan is die derde wel een verwerker. Die opdracht ziet in de kern immers wél op verwerking van persoonsgegevens.

Besteedt u de personeels- of loonadministratie uit aan een ander, dan zult u moeten nagaan of de verwerker in kwestie voldoet aan de wettelijke eisen omtrent de verwerking van persoonsgegevens. De bescherming van de rechten van betrokkenen, in dit geval de werknemers, moet zijn gewaarborgd. Er moeten daardoor passende technische en organisatorische maatregelen worden getroffen. Het is uw taak te controleren of de verwerker de zaken op orde heeft. Verder zult u een overeenkomst moeten sluiten met de verwerker, waarin u minimaal een aantal onderwerpen regelt en vastlegt. In de bijlage treft u hiervoor een voorbeeldovereenkomst aan. De geel gearceerde onderdelen zijn de onderwerpen waarvan de AVG voorschrijft dat u ze regelt.

Als werkgever hebt u natuurlijk ook te maken met de arbodienst, het UWV, de Belastingdienst en het verplicht gestelde bedrijfstakpensioenfonds (zoals PMT en PME). Al deze partijen hebben in de wet vastgelegde taken en daardoor eigen verplichtingen ten aanzien van (wettelijk voorgeschreven) verwerkingen. U bent wettelijk verplicht om deze partijen/overheidsinstanties bepaalde persoonsgegevens te verstrekken voor het in de wet vastgestelde doel. In het geval van de arbodienst geldt dat de arbodienst voor het medische deel van de verwerkingen de verwerkingsverantwoordelijke is. Dat bent u voor het medische deel dus niet zelf, omdat u niet degene bent die bepaalt hoe en waarvoor de medische gegevens precies worden verwerkt.

Om deze reden zijn de bovengenoemde partijen/overheidsinstanties géén verwerkers, maar verwerkingsverantwoordelijken. Zie ook de definitie uit paragraaf 1.1 van het algemene deel van deze serie:

"Verwerkingsverantwoordelijke: het bedrijf, de organisatie of de persoon/personen die bepaalt/bepalen waarvoor en hoe persoonsgegevens worden verwerkt.*"*

Dit betekent dat u - voor het verstrekken van persoonsgegevens van uw werknemers - met het UWV, de Belastingdienst en het verplicht gestelde bedrijfstakpensioenfonds geen verwerkersovereenkomst hoeft aan te gaan.

Dan kan zich nog de situatie voordoen dat u uw persoonsgegevens opslaat op servers die niet van u zijn, maar van een andere partij. Het gebruikmaken van deze serverruimte voor de opslag van persoonsgegevens is een opdracht die ziet op het verwerken van persoonsgegevens. Dat maakt dat de partij die de serverruimte ter beschikking stelt een verwerker is en u hiermee eveneens een verwerkersovereenkomst moet sluiten. U kunt hierbij bijvoorbeeld denken aan het bedrijf Microsoft. In het kader van Office 365 bijvoorbeeld wordt vaak gebruik gemaakt van opslagruimte van Microsoft voor e-mails in Outlook of voor bestanden in OneDrive. Het nadeel van een groot bedrijf als Microsoft is dat u hiermee hoogstwaarschijnlijk niet zult kunnen onderhandelen over een verwerkersovereenkomst. Bij de aanschaf van de gebruikslicentie zult u simpelweg met de contractuele voorwaarden van Microsoft moeten instemmen. Dat geldt ook voor persoonsgegevens die in handen komen van andere derden, zoals bijvoorbeeld de leveranciers van besturingssystemen (denk aan Windows). Vraag uw ICT'er in ieder geval te bekijken of er gegevensoverdracht plaatsvindt en de instellingen zo privacyvriendelijk mogelijk te maken. Voor Windows 10 heeft de AP een 'Handleiding privacyvriendelijk instellen Windows 10' opgesteld. Deze kunt u vinden op de website van de AP.

Kortom, de meeste mkb'ers zullen in ieder geval verwerkersovereenkomsten moeten sluiten met het bedrijf dat voor hen (delen van) de personeels- of loonadministratie beheert of uitvoert, met de externe partij op wiens server persoonsgegevens worden opgeslagen en met de arbodienst of bedrijfsarts die méér persoonsgegevens verzamelt en gebruikt dan alleen de medische gegevens (dit zal meestal wel het geval zijn).

Terug naar de checklist

BIJLAGEN

BIJLAGE 1 : PRIVACYVERKLARING

…Uw naam (incl. rechtsvorm) vestigingsadres…
…postcode, plaats…
…telefoonnummer en e-mailadres…

Verzamelen en gebruiken van persoonsgegevens van sollicitanten, uitzendkrachten/payroll-werknemers, stagiaires en werknemers.
Graag maken wij u er op attent dat wij de persoonsgegevens die u ons verstrekt zullen verzamelen en gebruiken omdat dit noodzakelijk is voor het doorlopen van de sollicitatieprocedure of om een (eventuele) arbeidsovereenkomst / stageovereenkomst / uitzendovereenkomst te sluiten en uit te voeren. Daarnaast zijn bepaalde persoonsgegevens nodig voor de nakoming en uitvoering van bepalingen uit de voor ons geldende CAO. Ook verzamelen en gebruiken wij uw persoonsgegevens om aan bepaalde wettelijke verplichtingen te kunnen voldoen. Deze wettelijke verplichtingen hebben bijvoorbeeld te maken met de vaststelling en verschuldigdheid van belastingen en premies voor werknemers.

Gelet op deze noodzaak bent u verplicht om de hiervoor benodigde persoonsgegevens aan ons te verstrekken. Als u ons geen of onvoldoende persoonsgegevens verstrekt, dan kunnen wij mogelijk geen sollicitatieprocedure met u doorlopen, een (eventuele) arbeidsovereenkomst / stageovereenkomst / uitzendovereenkomst met u aangaan en uitvoeren of aan onze wettelijke verplichtingen voldoen.

Bent u (payroll-)werknemer of stagiair, dan gebruiken wij uw gegevens voor het opstellen, uitvoeren en beëindigen van de arbeids- of stageovereenkomst of de arbeidsrelatie. Hieronder wordt onder meer verstaan:

a) de behandeling van personeelszaken;
b) het vaststellen en uitbetalen van het salaris, vergoedingen en andere geldbedragen; en
c) het vaststellen en betalen van eventuele belastingen, premies en andere fiscale verplichtingen ten behoeve van u als werknemer of stagiair.

Bent u een sollicitant, dan gebruiken wij uw gegevens om met u te kunnen communiceren over het verloop van de sollicitatieprocedure, de beoordeling van uw geschiktheid voor een functie die vacant is of kan komen en de eventuele afhandeling van de door u gemaakte onkosten.

Bent u een uitzendkracht, dan zullen wij de gegevens die wij verkrijgen van het uitzendbureau gebruiken voor de beoordeling van uw geschiktheid voor een functie die vacant is of kan komen en voor de uitvoering van de uitzendovereenkomst.

Doorgifte aan derden
Het is mogelijk dat wij uw persoonsgegevens doorgeven aan andere partijen. Deze andere partijen kunnen overheidsorganen zijn, maar ook partijen die in onze opdracht werkzaamheden uitvoeren of partijen aan wie wij verplicht zijn gegevens te verstrekken in verband met de (uitvoering van de) arbeidsovereenkomst. Het gaat om de volgende partijen: **[graag verder aanvullen of aanpassen]**

- de Belastingdienst;
- het UWV;
- onze arbodienst/bedrijfsarts;
- de Inspectie voor Sociale Zaken en Werkgelegenheid;
- het Pensioenfonds;
- de leasemaatschappij;
- de verzuimverzekeraar;
- onze accountant/boekhouder/salarisadministrateur;
- […]
- […]

Soms zal het verstrekken van uw gegevens aan een ander noodzakelijk zijn om te kunnen voldoen aan de wet, zoals het geval is bij doorgifte aan de Belastingdienst, het UWV, de arbodienst/bedrijfsarts, het (verplicht gestelde) Pensioenfonds en de Inspectie voor Sociale Zaken en Werkgelegenheid.

In andere gevallen is de doorgifte noodzakelijk om de (arbeids)overeenkomst met u te kunnen uitvoeren, zoals bij doorgifte aan de leasemaatschappij. Bij verstrekking van uw gegevens aan onze verzuimverzekeraar hebben wij een gerechtvaardigd belang, namelijk dat wij daardoor aanspraak kunnen maken op een verzekeringsuitkering.

Daarnaast zijn er partijen die in onze opdracht werkzaamheden uitvoeren, zoals de accountant/boekhouder/salarisadministrateur. Bij deze doorgifte van uw gegevens hebben wij een gerechtvaardigd belang. Deze werkzaamheden zijn uitbesteed vanwege (onder meer) de kennis en expertise die onze accountant/boekhouder/salarisadministrateur bezit. Om de (arbeids)overeenkomst met u uit te voeren, heeft de accountant/boekhouder/salarisadministrateur uw persoonsgegevens nodig.

Verder maken wij gebruik van externe serverruimte voor de opslag van (delen van) onze personeels- en loonadministratie, waar uw persoonsgegevens onderdeel van uitmaken. Uw persoonsgegevens worden om die reden aan onze serverprovider verstrekt. Daarnaast maken wij gebruik van Microsoft Office en de bijbehorende opslagmogelijkheden voor e-mails en andere bestanden. Wij hebben bij deze twee doorgiften een gerechtvaardigd belang, omdat wij gegevens digitaal willen opslaan en verwerken en uitbesteding hiervan verschillende voordelen heeft.

Bewaarperiode persoonsgegevens
Wij zullen uw sollicitatiegegevens uiterlijk 4 weken na het eindigen van de sollicitatieprocedure verwijderen, tenzij u ons toestemming heeft gegeven om uw gegevens voor een periode van maximaal 1 jaar te bewaren.

De persoonsgegevens uit de salarisadministratie die fiscaal van belang zijn zullen wij bewaren gedurende een periode van 7 jaar nadat u uit dienst bent getreden. Deze bewaartermijn hangt samen met een voor ons geldende wettelijke verplichting. Loonbelastingverklaringen en een kopie van uw identiteitsbewijs zullen wij 5 jaar na het einde van uw dienstverband bewaren. Ook deze bewaartermijn hangt samen met een voor ons geldende wettelijke verplichting.

Voor andere gegevens uit de personeels- of loonadministratie hanteren wij een bewaartermijn van uiterlijk 2 jaar nadat uw dienstverband is beëindigd, tenzij blijkt dat bepaalde persoonsgegevens voor ons noodzakelijk zijn om te voldoen aan een wettelijke (bewaar)plicht of als sprake is van een arbeidsconflict of rechtszaak. Bij 'andere gegevens uit de personeels- of loonadministratie' moet u bijvoorbeeld denken aan arbeidsovereenkomsten, verslagen van beoordelings- en functioneringsgesprekken, correspondentie over benoeming, promotie, degradatie en ontslag, getuigschriften en administratieve verzuimgegevens.

Uw rechten
U heeft het recht om ons te vragen om uw eigen persoonsgegevens te mogen inzien. Als daartoe aanleiding bestaat, kunt u ons ook verzoeken om aanvulling van uw persoonsgegevens of om het wijzigen van onjuistheden. Daarnaast heeft u het recht om te vragen om uw persoonsgegevens te wissen of het gebruik van uw persoonsgegevens te beperken. Ook kunt u bij ons bezwaar maken tegen het verzamelen en gebruiken van uw gegevens. Vindt u dat wij onjuist omgaan met uw persoonsgegevens dan kunt u hierover een klacht indienen bij de organisatie die toezicht houdt op de privacyregels, de Autoriteit Persoonsgegevens. Tot slot kunt u ons verzoeken om verkrijging van uw persoonsgegevens of overdracht van die gegevens aan een ander.

U kunt de hierboven genoemde rechten niet onder alle omstandigheden uitoefenen. Hebben wij uw persoonsgegevens bijvoorbeeld nodig om de wet na te leven, dan kunt u geen bezwaar maken of verzoeken om wissing.

Om uw rechten te kunnen uitoefenen kunt u zich wenden tot: **(...uw bedrijfsnaam / specifieke contactpersoon van uw bedrijf, adres, postcode, plaats, telefoonnummer en e-mailadres...)**. Ook met vragen of voor meer informatie over het verzamelen en gebruiken van uw persoonsgegevens kunt u uiteraard contact met ons opnemen.

BIJLAGE 2 : VERWERKERSOVEREENKOMST

Terug naar de checklist

Deze overeenkomst is geschreven vanuit het perspectief van de verwerkingsverantwoordelijke. Bent u zelf verwerker, dan kunt u beter een andere modelovereenkomst gebruiken. Neemt u daarvoor contact op met Bedrijfsjuridisch Ledenadvies van Metaalunie.

In deze verwerkersovereenkomst worden alleen de wederzijdse rechten en plichten geregeld zoals deze uit de AVG voortvloeien. Verwerkingen zullen echter vaak plaatsvinden in het kader van een opdracht aan een ander, bijvoorbeeld het uitbesteden van de loonadministratie. De niet-privacygerelateerde aspecten van uw relatie met de verwerker worden in deze overeenkomst niet geregeld. Denkt u hierbij aan contractuele aspecten zoals de inhoud van de opdracht, de duur daarvan, de vergoeding die de ander krijgt, etc. U kunt hiervoor eventueel gebruik maken van een andere overeenkomst. Neem contact op met één van de adviseurs van Bedrijfsjuridisch Ledenadvies om te bespreken wat voor soort modelovereenkomst van ons u hiervoor kunt gebruiken.

Ondergetekenden,

de (**besloten vennootschap (naam) B.V**.), gevestigd te (**plaatsnaam**), ingeschreven bij de Kamer van Koophandel onder nummer (**nummer**) en hierbij vertegenwoordigd door haar directeur (**naam**),
verder te noemen "**Verwerkingsverantwoordelijke**"

en

de (**besloten vennootschap (naam) B.V.**), gevestigd te (**plaatsnaam**), ingeschreven bij de Kamer van Koophandel onder nummer (**nummer**) en hierbij vertegenwoordigd door haar directeur (**naam**),
hierna te noemen "**Verwerker**";

Verwerkingsverantwoordelijke en Verwerker hierna gezamenlijk te noemen: "Partijen";

in aanmerking nemende dat:

- Verwerkingsverantwoordelijke een onderneming drijft die zich bezighoudt met (**omschrijf de werkzaamheden van de Verwerkingsverantwoordelijke**);
- Verwerker een onderneming drijft die zich bezighoudt met (**omschrijf de werkzaamheden van de Verwerker**);
- Verwerkingsverantwoordelijke de volgende activiteiten wenst uit te besteden aan Verwerker, namelijk: (**vul in welke verwerkingsactiviteiten Verwerker gaat uitvoeren, bijv. opslag van persoonsgegevens in de cloud**);
- de genoemde activiteiten betrekking hebben op verwerkingen van persoonsgegevens en partijen daarom verplicht zijn met elkaar een verwerkersovereenkomst willen sluiten.
- Partijen hun rechten en plichten in hun hoedanigheid van Verwerker en Verwerkingsverantwoordelijke nader wensen vast te leggen;

verklaren als volgt te zijn overeengekomen:

Artikel 1: Verwerkingsactiviteiten

1. Verwerkingsverantwoordelijke verleent aan Verwerker de opdracht tot het uitvoeren van de volgende verwerkingsactiviteiten: (**hier benoemen welke verwerkingsactiviteiten worden uitbesteed aan Verwerker**), hierna te noemen de "verwerkingsactiviteiten".
2. De verwerkingen die zullen plaatsvinden en het doel van die verwerkingen kunnen als volgt worden gespecificeerd: (**invullen**).
3. De categorieën van personen wiens gegevens worden verwerkt zijn: (**invullen**).
4. Het soort persoonsgegevens dat Verwerker gaat verwerken is: (**invullen**).

Artikel 2: Algemene verplichtingen Verwerker

1. Verwerker zal de persoonsgegevens uitsluitend verwerken op basis van schriftelijke instructies van Verwerkingsverantwoordelijke.
2. Als Verwerker wettelijk verplicht is persoonsgegevens afkomstig van Verwerkingsverantwoordelijke te verwerken, dan stelt Verwerker Verwerkingsverantwoordelijke voorafgaand aan de

verwerking in kennis van het wettelijk voorschrift dat haar hiertoe verplicht. Deze kennisgeving mag achterwege blijven als zij verboden is vanwege gewichtige redenen van algemeen belang.

3. Verwerker waarborgt dat de personen die de persoonsgegevens verwerken vertrouwelijkheid in acht nemen door hen schriftelijk tot geheimhouding te verplichten. Op eerste verzoek van Verwerkingsverantwoordelijke is Verwerker verplicht aan te tonen dat hij aan deze verplichting heeft voldaan.

Artikel 3: Beveiliging

1. Verwerker neemt passende technische en organisatorische maatregelen om te waarborgen dat de persoonsgegevens zijn beveiligd. Het beveiligingsniveau moet zijn afgestemd op het risico c.q. de risico's die verwerking van de persoonsgegevens met zich meebrengt/meebrengen.
2. Verwerker zal minimaal de in Bijlage 1 opgenomen beveiligingsmaatregelen treffen.

Artikel 4: Vrijwaring

1. Verwerker vrijwaart Verwerkingsverantwoordelijke voor alle aanspraken van derden, waaronder in ieder geval personen van wie gegevens zijn verwerkt alsmede de Autoriteit Persoonsgegevens, die voortvloeien uit of verband houden met het niet of onvoldoende naleven van de verplichtingen uit deze overeenkomst of de op grond van artikel 2, eerste lid, gegeven schriftelijke instructies.

Artikel 5: Uitbesteding verwerkingsactiviteiten

1. Zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke is het Verwerker niet toegestaan (delen van) de verwerkingsactiviteiten uit te besteden aan een andere partij (hierna te noemen "subverwerker").
2. Als Verwerker toestemming krijgt van Verwerkingsverantwoordelijke om een derde in te schakelen bij de uitvoering van de verwerkingsactiviteiten dan is Verwerker gehouden door middel van een schriftelijke overeenkomst de verplichtingen die in de onderhavige overeenkomst aan haar zijn opgelegd eveneens aan haar subverwerker op te leggen.

Artikel 6: Bijstand

1. Verwerker zal Verwerkingsverantwoordelijke alle bijstand verlenen die Verwerkingsverantwoordelijke noodzakelijk acht om:
   a. te kunnen antwoorden op verzoeken van betrokkenen tot uitoefening van hun rechten. Verwerker treft passende technische en organisatorische maatregelen om deze verplichting onverwijld tegenover Verwerkingsverantwoordelijke te kunnen nakomen;
   b. passende technische en organisatorische maatregelen te treffen om een op de risico's afgestemd beveiligingsniveau te waarborgen;
   c. te kunnen voldoen aan alle wettelijke verplichtingen omtrent de gegevensbeschermingseffectbeoordeling en de eventuele voorafgaande raadpleging van de Autoriteit Persoonsgegevens die daarvan het gevolg kan zijn;
   d. te kunnen beoordelen of incidenten een datalek opleveren die bij de Autoriteit Persoonsgevens en/of de betrokkenen gemeld moeten worden, de melding(en) op te stellen, maatregelen te nemen tot beperking en voorkoming van (verdere) inbreuken en schade en al het overige te doen waartoe zij in verband met de wettelijke bepalingen omtrent datalekken verplicht is.
2. Onder het verlenen van bijstand als bedoeld in dit artikel wordt in ieder geval (maar niet uitsluitend) verstaan: het verstrekken van (schriftelijke of elektronische) informatie, het treffen van technische en organisatorische maatregelen en het toegang geven tot de plaats of plaatsen waar de verwerkingsactiviteiten worden uitgevoerd.

Artikel 7: Einde van de overeenkomst

1. Bij het einde van deze overeenkomst dient Verwerker onmiddellijk alle persoonsgegevens **aan Verwerkingsverantwoordelijke terug te bezorgen/te wissen***, en bestaande kopieën te verwijderen, tenzij opslag van de persoonsgegevens wettelijk verplicht is.
   ***verwijderen wat niet van toepassing is.**

Artikel 8: Plicht tot informatievoorziening

1. Verwerker zal Verwerkingsverantwoordelijke alle informatie ter beschikking stellen die nodig is om te kunnen aantonen dat aan de verplichtingen uit de Algemene Verordening Gegevensbescherming en de Uitvoeringswet Algemene verordening gegevensbescherming is voldaan. Ook zal hij alle informatie ter beschikking stellen die nodig is om audits en inspecties mogelijk te maken en daaraan bij te dragen.

Artikel 9: Nederlands recht en bevoegde rechter

1. Op deze overeenkomst is Nederlands recht van toepassing.
2. De burgerlijke rechter die bevoegd is in de vestigingsplaats van Verwerkingsverantwoordelijke neemt kennis van geschillen. Verwerkingsverantwoordelijke mag van deze bevoegdheidsregel afwijken en de wettelijke bevoegdheidsregels hanteren.

Aldus overeengekomen en in tweevoud opgemaakt op (**invullen datum**) te (**invullen plaats**)

Namens Verwerkingsverantwoordelijke	Namens Verwerker
Handtekening	*Handtekening*
Naam:	Naam:
Functie:	Functie:

Bijlage 1 : Lijst van beveiligingsmaatregelen (per soort persoonsgegeven)

BIJLAGE 3 : VRAGENLIJST T.B.V. DOCUMENTATIE INCIDENTEN

Terug naar de checklist

1. Geef een samenvatting van het incident. Wees zo volledig mogelijk in het omschrijven van de feiten en omstandigheden.

2. Is er sprake geweest van een dreiging of tekortkoming in de beveiliging of zijn er daadwerkelijk persoonsgegevens betrokken bij het incident (bijv. persoonsgegevens zijn verloren gegaan of vernietigd, toegankelijk gemaakt of verstrekt aan een ander die deze gegevens niet zou mogen hebben).

3. Als er persoonsgegevens betrokken zijn bij het incident, om hoeveel personen gaat het dan? (*Vul de aantallen in.*)
   a) Minimaal: (**vul aan**)
   b) Maximaal: (**vul aan**)

4. Omschrijf de groep mensen van wie persoonsgegevens betrokken zijn bij het incident.

5. Wanneer vond het incident plaats?
   (*Kies een van de volgende opties en vul waar nodig aan.*)
   a) Op (**datum**)
   b) Tussen (**begindatum periode**) en (**einddatum periode**)
   c) Nog niet bekend

6. Wat is de aard van het incident?
   - (Lezen (vertrouwelijkheid),
   - Kopiëren,
   - Veranderen (integriteit),
   - Verwijderen of vernietigen (beschikbaarheid),
   - Diefstal,
   - Nog niet bekend.

7. Om welk type persoonsgegevens gaat het? (U kunt meerdere mogelijkheden aankruisen.)
   a) Naam-, adres- en woonplaatsgegevens
   b) Telefoonnummers
   c) E-mailadressen of andere adressen voor elektronische communicatie
   d) Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord of klantnummer)
   e) Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
   f) Burgerservicenummer (BSN) of sofinummer
   g) Paspoortkopieën of kopieën van andere legitimatiebewijzen
   h) Geslacht, geboortedatum en/of leeftijd
   i) Bijzondere persoonsgegevens (bijvoorbeeld ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens)
   j) Overige gegevens, namelijk (**vul aan**)

8. Welke gevolgen kan het incident hebben voor de persoonlijke levenssfeer van de betrokkenen? (*U kunt meerdere mogelijkheden aankruisen.*)
   a) Stigmatisering of uitsluiting
   b) Schade aan de gezondheid
   c) Blootstelling aan (identiteits)fraude
   d) Blootstelling aan spam of phishing
   e) Anders, namelijk (**vul aan**)

9. Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om het incident aan te pakken en om verdere inbreuken te voorkomen?

10. Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen? (*Kies een van de volgende opties.*)
    a) Ja
    b) Nee
    c) Nog niet bekend

11. Wanneer heeft u het datalek gemeld aan de betrokkenen, of wanneer gaat u dit doen? (*Beantwoord deze vraag als u vraag 10 met ja hebt beantwoord. Kies een van de volgende opties en vul waar nodig aan.*)
    a) Ik heb het datalek aan de betrokkenen gemeld op (**datum**)
    b) Ik ga het datalek aan de betrokkenen melden op (**datum**)
    c) Nog niet bekend

12. Wat is de inhoud van de melding aan de betrokkenen? (*Letterlijke weergave, beantwoord deze vraag als u vraag 10 met ja hebt beantwoord.)*

13. Hoeveel betrokkenen heeft u in kennis gesteld of gaat u in kennis stellen? (*Beantwoord deze vraag als u vraag 10 met ja hebt beantwoord.*)

14. Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken bij het in kennis stellen van de betrokkenen? (*Beantwoord deze vraag als u vraag 10 met ja hebt beantwoord.*)

15. Waarom ziet u af van het melden van het datalek aan de betrokkenen? (*Beantwoord deze vraag als u vraag 10 met nee hebt beantwoord. Kies een van de onderstaande opties en vul waar nodig aan.*)
    a) De technische beschermingsmaatregelen die ik heb getroffen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten;
    b) Het is onwaarschijnlijk dat het datalek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, want: (**vul aan**)
    c) Ik heb zwaarwegende redenen om de melding aan de betrokkene achterwege te laten, namelijk: (**vul aan**)
    d) Anders, namelijk: (**vul aan**)

16. Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden? (*Kies een van de volgende opties en vul waar nodig aan.*)
    a) Ja
    b) Nee
    c) Deels, namelijk: (**vul aan**)

17. Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? (*Beantwoord deze vraag als u bij vraag 16 gekozen heeft voor optie a of optie c. Als u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.*)

18. Heeft de inbreuk betrekking op personen in andere EU-landen? (*Kies een van de volgende opties.*)
    a) Ja
    b) Nee
    c) Nog niet bekend

19. Heeft uw bedrijf of organisatie het datalek gemeld bij toezichthouders in een of meer andere EU-landen?
    a) Ja, namelijk: (**vul aan**)
    b) Nee

BIJLAGE 4 : REGISTER VOOR VERWERKINGSACTIVITEITEN

Terug naar de tekst

Voor de verwerkingsverantwoordelijke:

	Verwerkingsactiviteiten ten aanzien van persoonsgegevens	
1	Voor welk administratief onderdeel worden persoonsgegevens verwerkt	
2	Naam en contactgegevens verwerkingsverantwoordelijke, diens vertegenwoordiger* en de FG	
3	Doel(en) verwerking	
4	Van welke categorieën personen worden gegevens verwerkt	
5	Welke categorieën persoonsgegevens worden verwerkt	
6	Aan welke categorieën ontvangers zijn of zullen de persoonsgegevens worden verstrekt	
7	Aan welk land of aan welke organisatie buiten de EER gaat u persoonsgegevens doorgeven en (indien van toepassing) uit welke documenten blijkt welke passende waarborgen er zijn ter bescherming van de persoonsgegevens	
8	Hoe lang gaat u de persoonsgegevens bewaren	
9	Welke beveiligingsmaatregelen zijn er getroffen	

* Onder 'vertegenwoordiger' wordt verstaan de persoon of partij die in de EER is aangewezen om een buiten de EER gevestigde verwerkingsverantwoordelijke of verwerker te vertegenwoordigen. De meeste Metaalunieleden zullen dit kunnen verwijderen uit het register, omdat zij zelf binnen de EER zitten en dus geen vertegenwoordiger nodig hebben.

Voor een toelichting op punt 7: zie Hoofdstuk 6 van het Algemene deel in deze serie

Voor de verwerker:

	Verwerkingsactiviteiten ten aanzien van persoonsgegevens	
1	Naam en contactgegevens verwerker, verwerkingsverantwoordelijke en de FG	
2	De categorieën van verwerkingen die voor rekening van de verwerkingsverantwoordelijke worden uitgevoerd	
3	Aan welk land of aan welke organisatie buiten de EER gaat u persoonsgegevens doorgeven en (indien van toepassing) uit welke documenten blijkt welke passende waarborgen er zijn ter bescherming van de persoonsgegevens	
4	Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen die zijn getroffen	

Voor een toelichting op punt 3: zie Hoofdstuk 6 van het Algemene deel in deze serie

Bovenstaande voorbeeldregisters in de vorm van een Excel bestand ontvangen? Neem contact op met Bedrijfsjuridisch Ledenadvies: 030-6053344 of bj@metaalunie.nl.