Metaalunie-serie:

DE ALGEMENE VERORDENING GEGEVENSBESCHERMING

Algemeen deel en Deel 1: Klant- en leveranciersbeheer

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 4

ALGEMEEN DEEL 5

Hoofdstuk 1: Begrippen, grondslagen en beginselen 6

§ 1.1. Algemeen 6
§ 1.2. Grondslagen 6
§ 1.3 Algemene beginselen voor de verwerking van persoonsgegevens 7

Hoofdstuk 2: Beveiliging 8

§ 2.1 Passende maatregelen treffen 8
§ 2.2 Datalekken 9
§ 2.3 Documentatieplicht voor incidenten 10

Hoofdstuk 3: De rechten van betrokkenen 11

§ 3.1 Termijn 11
§ 3.2 Recht van inzage 11
§ 3.3 Recht op rectificatie 11
§ 3.4 Recht op wissing 12
§ 3.5 Recht op beperking van de verwerking 12
§ 3.6 Recht op overdraagbaarheid 12
§ 3.7 Recht van bezwaar 13
§ 3.8 In kennis stellen van derden over uitoefening rechten 14

Hoofdstuk 4: De functionaris voor gegevensbescherming 15

Hoofdstuk 5: De gegevensbeschermingseffectbeoordeling 16

Hoofdstuk 6: Het doorgeven van persoonsgegevens aan derden 18

Hoofdstuk 7: Het register voor verwerkingsactiviteiten 19

§ 7.1 Wat houdt de registratieplicht in 19
§ 7.2 Uitzonderingen op de registratieplicht 19
§ 7.3 Hoe te voldoen aan de registratieplicht 20

Hoofdstuk 8: Verantwoordingsplicht (‘accountability’) 21

DEEL 1: KLANT- EN LEVERANCIERSBEHEER 22

Hoofdstuk 1: Het profiel van metaalbedrijf Jansen ten aanzien van klant- en leveranciersbeheer 23

Hoofdstuk 2: Lijst van actiepunten 25

Hoofdstuk 3: Toelichting op de actiepuntenlijst 30

§ 3.1 Verwerking persoonsgegevens 30
§ 3.2 Informatie die u moet verstrekken 31
§ 3.3 De wijze en het moment waarop de informatie moet worden verstrekt 34
§ 3.4 Direct marketing 36
§ 3.5 Toestemming vragen 37
§ 3.6 Bewaartermijn 39
§ 3.7 Verwerkingsactiviteiten uitbesteden 39

BIJLAGEN 41

BIJLAGE 1 : VERWERKERSOVEREENKOMST 42
BIJLAGE 2 : VRAGENLIJST T.B.V. DOCUMENTATIE INCIDENTEN 45
BIJLAGE 3 : REGISTER VOOR VERWERKINGSACTIVITEITEN 47
BIJLAGE 4 : PRIVACYVERKLARING (BIJGEWERKT TOT EN MET DEEL 1) 48

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: 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

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.

§ 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 2 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.

§ 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. Het bestand dat u dan 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 gaat behoorlijk ver. Van u wordt verwacht dat de betrokkene de persoonsgegevens zelf moet kunnen downloaden. Bijvoorbeeld via een tool waarmee uw klanten hun gegevens direct op een beveiligde manier kunnen downloaden. Ook moet u ervoor zorgen dat uw klanten hun gegevens direct kunnen doorgeven aan een andere organisatie. Dit kunt u bijvoorbeeld doen met een *application programming interface* (API), waarmee u een verbinding mogelijk maakt tussen uw systeem of applicatie en dat van een andere partij.

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.

Wij zijn van mening dat bovenstaande voor het mkb wellicht weinig werkbaar is en mogelijk allerlei ICT-investeringen vraagt. Wij houden de publicaties van de AP in de gaten en hopen van deze instantie meer te horen over een laagdrempelige, praktische en werkbare manier voor het midden- en kleinbedrijf om betrokkenen in staat te stellen hun recht op overdraagbaarheid te kunnen uitoefenen. Zodra wij meer weten, zullen wij u hierover inlichten.

§ 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 privacy 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.

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

§ 7.3 Hoe te voldoen aan de registratieplicht

Om aan de AVG te voldoen, adviseren wij u om al uw verwerkingsactiviteiten te registreren. In bijlage 3 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

U zult er uiteraard ook voor moeten zorgen dat het register actueel wordt gehouden. Het is verstandig hiervoor binnen uw bedrijf een procedure in het leven te roepen.

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 1: KLANT- EN LEVERANCIERSBEHEER

Hoofdstuk 1: Het profiel van metaalbedrijf Jansen ten aanzien van klant- en leveranciersbeheer

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 klant- en leveranciersbeheer. Hieronder verstaan wij alle bestanden, toepassingen en programma's die betrekking hebben op bestellingen, leveringen, factureren enz. Als synoniem voor klantbeheer gebruiken wij ook wel de begrippen "klant-" of "verkoopadministratie". Voor leveranciersbeheer worden ook wel de begrippen "leveranciers-"of "inkoopadministratie" gebruikt.

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 levert zaken en diensten aan consumenten (B2C), maar ook aan bedrijven en organisaties (B2B).
- ○ Metaalbedrijf Jansen koopt zaken en diensten in van bedrijven en organisaties (B2B).
- ○ De persoonsgegevens hebben betrekking op potentiële, bestaande of oude klanten en leveranciers.
- ○ Metaalbedrijf Jansen verwerkt persoonsgegevens op geautomatiseerde wijze, wat wil zeggen dat zij met behulp van één of meerdere computers persoonsgegevens opslaat, bewerkt, etc. Met andere woorden: de klantadministratie en leveranciersadministratie wordt digitaal beheerd.
- ○ Metaalbedrijf Jansen verwerkt géén bijzondere persoonsgegevens (zie de definitie van de bijzondere persoonsgegevens zoals besproken in §1.1).
- ○ De persoonsgegevens zijn afkomstig van de klanten of de leveranciers zelf, metaalbedrijf Jansen heeft ze niet van derden verkregen of gekocht.
- ○ Metaalbedrijf Jansen maakt gebruik van Microsoft Windows en Microsoft Office.
- ○ De gegevens worden niet gekoppeld aan of samengevoegd met andere gegevens van de klant of leverancier die op een ander moment en/of in een andere context zijn verkregen, waardoor metaalbedrijf Jansen nog meer weet van de desbetreffende personen.
- ○ 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 voor meer informatie.
- ○ Daarnaast komen de verwerkingen niet neer op het volgen van de locatie of de verplaatsingen van personen.
- ○ Zij stelt met behulp van de persoonsgegevens geen profielen op van de betrokkenen om een beeld te krijgen van bijvoorbeeld hun interesses, gedrag of economische situatie, en dergelijke.
- ○ Metaalbedrijf Jansen verstrekt de persoonsgegevens van haar klanten en leveranciers alleen aan andere leveranciers en opdrachtnemers in het kader van het uitbesteden van werkzaamheden en het inkopen van zaken zoals materialen, onderdelen en eindproducten.
- ○ Metaalbedrijf Jansen doet aan direct marketing. Zij stuurt reclamemailings aan haar bestaande klanten en maakt daarbij gebruik van een nieuwsbrief mailing dienst.
- ○ Metaalbedrijf Jansen communiceert met haar (potentiële) klanten en leveranciers en sluit overeenkomsten met hen per e-mail, schriftelijk en telefonisch.

- ○ 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. klant- en leveranciersbeheer aan de Algemene Verordening Gegevensbescherming te voldoen.

Vind-plaats toe-licht-ing	Actiepunten	Uitge-voerd
KLANT- EN LEVERANCIERSBEHEER (profiel metaalbedrijf Jansen, zie hoofdstuk 1 van deel 1)		
Hfd. 4 (alg deel)	Ga na of u een functionaris voor gegevensbescherming moet aanstellen. Dit hoeft u in principe eenmalig te doen (tenzij uw situatie verandert uiteraard) en dit onderwerp zal daarom in de volgende delen van deze serie niet meer aan de orde komen.	
Hfd. 5 (alg deel)	Ga na of er verwerkingen binnen uw klant- en leveranciersadministratie plaats-vinden waarvoor u een DPIA (een gegevensbeschermingseffectbeoordeling) moet uitvoeren.	
§ 3.2 (deel 1)	Stel een privacyverklaring op waarin u uw klanten en leveranciers informeert over de onderwerpen waarover u hen moet informeren. U kunt hiervoor de onderstaande tekst gebruiken: ***PRIVACYVERKLARING*** ***Verzamelen en gebruiken van persoonsgegevens van klanten, leveranciers en andere opdrachtnemers*** *Graag maken wij u er op attent dat wij de persoonsgegevens die u ons verstrekt zullen verzamelen en gebruiken omdat dit noodzakelijk is om een eventuele overeenkomst met u te sluiten en uit te voeren. Dat geldt zowel voor onze (potentiële) klanten als voor partijen bij wie wij zaken en/of diensten inkopen.* *Bent u een (potentiële) klant van ons, dan gebruiken wij uw gegevens om u een offerte te kunnen toesturen, te kunnen bepalen aan welke specificaties of wensen een bepaalde zaak of dienst dient te voldoen, zaken te kunnen leveren of werkzaamheden voor u te kunnen verrichten, te kunnen factureren en met u vlot en efficiënt te kunnen communiceren over de uitvoeringsaspecten van de overeenkomst.* *Bent u een (potentiële) leverancier of andere opdrachtnemer dan zijn uw persoonsgegevens eveneens noodzakelijk voor de sluiting en uitvoering van de overeenkomst. Bij inkoop is dat nodig om u te kunnen laten weten aan welke specificaties of wensen een bepaalde zaak of dienst wat ons betreft dient te voldoen, een offerte-aanvraag te kunnen toesturen of een bestelling bij u te kunnen plaatsen, uw facturen te kunnen betalen en vlot en efficiënt met u te kunnen communiceren over andere aspecten van de overeenkomst.* *U bent niet verplicht om ons uw persoonsgegevens te verstrekken. Als u ons geen of onvoldoende persoonsgegevens verstrekt, dan is het echter wel mogelijk dat wij aan de hiervoor genoemde werkzaamheden geen uitvoering kunnen geven.* ***Doorgifte aan derden*** *In verband met de uitvoering van een eventuele overeenkomst met u is het mogelijk dat wij uw persoonsgegevens moeten verstrekken aan partijen die onderdelen, materialen en producten aan ons toeleveren of in onze opdracht werkzaamheden uitvoeren. Verder maken wij gebruik*	

		van externe serverruimte voor de opslag van (delen van) onze verkoop- en inkoopadministratie, waar uw persoonsgegevens een onderdeel van uitmaken. Uw persoonsgegevens worden om die reden aan onze provider van serverruimte verstrekt. Omdat wij gebruik maken van een nieuwsbrief mailing dienst, worden uw persoonsgegevens tot slot doorgegeven aan de aanbieder van deze dienst. ***Direct marketing*** ***OPTIE 1 (als u onderscheid maakt tussen eenmalige klanten en klanten met wie u een duurzame relatie heeft en u alleen de klanten gaat mailen met wie u een duurzame relatie heeft):*** *Als u regelmatig bij ons bestelt, zullen wij de door u opgegeven persoonsgegevens bewaren en gebruiken om u in de toekomst persoonlijk per e-mail op de hoogte te brengen van onze bestaande en nieuwe producten en diensten en u hier eventueel een aanbieding voor te doen. Wij hebben bij het gebruik van uw persoonsgegevens voor dit doel een gerechtvaardigd belang, namelijk het aan de man brengen van onze producten en diensten. Iedere keer dat wij u een reclamemailing sturen, heeft u de mogelijkheid ons te laten weten hier geen prijs meer op te stellen. Zie hiervoor de afmeldlink onderaan iedere mailing.* *Bent u eenmalig klant bij ons, dan zullen wij u alleen reclameberichten toesturen als u ons daar vooraf uw toestemming voor heeft gegeven.* ***OPTIE 2 (als u géén onderscheid maakt tussen eenmalige klanten en klanten met wie u een duurzame relatie heeft en u daarom al uw klanten om toestemming voor direct marketing vraagt):*** *Als u ons daarvoor toestemming heeft gegeven, zullen wij de door u opgegeven persoonsgegevens bewaren en gebruiken om u in de toekomst persoonlijk per e-mail op de hoogte te brengen van onze bestaande en nieuwe producten en diensten en u hier eventueel een aanbieding voor te doen. Iedere keer dat wij u een reclamemailing sturen, heeft u de mogelijkheid ons te laten weten hier geen prijs meer op te stellen. Zie hiervoor de afmeldlink onderaan iedere mailing.* ***Bewaarperiode persoonsgegevens*** *Indien u een offerte bij ons heeft opgevraagd maar u geen klant bij ons geworden bent, zullen wij uw gegevens uiterlijk één jaar na ons laatste contact verwijderen. Ook indien wij een offerte van u hebben ontvangen, maar wij geen klant van u zijn geworden, zullen uw persoonsgegevens uiterlijk één jaar na ons laatste contact worden verwijderd. Bent u wel klant bij ons geworden of wij bij u, dan zullen wij uw persoonsgegevens bewaren voor de duur van zeven jaar na het einde van het boekjaar waarin de overeenkomst met u volledig is uitgevoerd. De periode van zeven jaar komt overeen met de periode waarbinnen wij verplicht zijn onze administratie te bewaren voor de Belastingdienst. Na afloop van deze periode zullen wij uw persoonsgegevens verwijderen.* ***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 of een klacht indienen bij de Autoriteit Persoonsgegevens. Tot slot kunt u ons verzoeken om verkrijging van uw persoonsgegevens of overdracht van die gegevens aan een ander. 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.*	

§ 3.3 (deel 1)	Verwijs nieuwe klanten en leveranciers bij het eerste contact naar uw privacyverklaring en verstrek hen een exemplaar. Bij klanten zal het eerste contactmoment veelal het toezenden van de offerte zijn, en bij leveranciers zal dat dat moment veelal het aanvragen van een offerte, of bij het plaatsen van een bestelling zijn. Hoe u precies naar uw privacyverklaring moet verwijzen hangt af van de manier waarop u met hen communiceert. Bij zaken doen via de e-mail kunt u 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. Wij verwijzen u graag naar www.metaalbedrijfjansen.nl/privacyverklaring (hyperlink) voor meer informatie over de verwerking van uw persoonsgegevens en de rechten die u heeft.* *(**OPTIONEEL: alleen opnemen als u bestaande klanten met wie u een duurzame relatie heeft op basis van een gerechtvaardigd belang mailings gaat versturen over soortgelijke producten of diensten**): Heeft u er bezwaar tegen dat wij uw e-mailadres gaan gebruiken voor het versturen van reclamemailings, laat ons dat dan weten. Afmelden voor dit soort berichten kan eenvoudig en kosteloos via de volgende link: [hyperlink invoegen]. Mocht de hyperlink onverhoopt niet werken, neemt u dan contact met ons op via: info@metaalbedrijfjansen.nl of op telefoonnummer: 012-345 67 89.* Bij schriftelijk (per post) zaken doen kunt u 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 deze privacyverklaring treft u in de bijlage aan.* *(**OPTIONEEL: alleen opnemen als u bestaande klanten met wie u een duurzame relatie heeft op basis van een gerechtvaardigd belang mailings gaat versturen over soortgelijke producten of diensten**): Heeft u er bezwaar tegen dat wij uw e-mailadres gaan gebruiken voor het versturen van reclamemailings, laat ons dat dan weten. Afmelden voor dit soort berichten kan eenvoudig en kosteloos via de volgende link: [hyperlink invoegen]. Mocht de hyperlink onverhoopt niet werken, neemt u dan contact met ons op via: info@metaalbedrijfjansen.nl of op telefoonnummer: 012-345 67 89.* Stuurt u daadwerkelijk een kopie van de privacyverklaring mee en maak er verder bij de opsomming van de eventuele bijlage(en) melding van dat u een kopie meestuurt. Bij telefonisch zakendoen: Voldoe mondeling aan uw informatieplicht en laat het telefoongesprek opvolgen door een e-mail of brief waarin u één van de hierboven genoemde verwijzingen naar uw privacyverklaring opneemt.	
§ 3.3 (deel 1)	Plaats een hyperlink op uw website die op iedere webpagina duidelijk zichtbaar is. Bijvoorbeeld in de header of de footer van uw website, onder de noemer: "Privacyverklaring" of "Privacy statement". Eventueel kunt u de privacyverklaring alvast een aantal keer uitprinten en klaarleggen om mee te sturen met het eerste schriftelijke document aan een klant/leverancier.	
§ 3.4 en § 3.5 (deel 1)	Vraag in de eerste e-mail of brief die u de klant stuurt toestemming voor verwerking van zijn persoonsgegevens voor direct marketing. Bij zaken doen per e-mail: In het eerste elektronische bericht dat u aan de klant stuurt, vraagt u hem om	

	toestemming voor verwerking van zijn persoonsgegevens voor direct marketing. U kunt hiervoor de volgende tekst gebruiken: *Wij willen u er in het bijzonder op attent maken dat wij uw persoonsgegevens in de toekomst graag willen gebruiken voor het toesturen van informatie over onze producten en diensten en het eventueel doen van aanbiedingen. In de privacyverklaring op onze website kunt u hier meer over lezen onder het kopje "Direct marketing". Zie hiervoor* www.metaalbedrijfjansen.nl/privacyverklaring. *Graag vernemen wij of u toestemming geeft voor het gebruik van uw persoonsgegevens voor dit doel. U kunt ons uw toestemming geven door een reply te sturen op deze e-mail en in deze reply de volgende zin over te nemen (dat kan eenvoudig met de kopieer- en plakfunctietoetsen):* *"Ja, ik ga akkoord met verwerking van mijn persoonsgegevens t.b.v. direct marketing zoals is omschreven in uw privacyverklaring."* *Uiteraard kunt u uw toestemming te allen tijde weer intrekken.* Bij schriftelijk zaken doen, kunt u de volgende tekst opnemen in uw eerste schriftelijke stuk gericht aan de klant: *Wij willen u er in het bijzonder op attent maken dat wij uw persoonsgegevens in de toekomst graag willen gebruiken voor het toesturen van informatie over onze producten en diensten en het eventueel doen van aanbiedingen. In onze privacyverklaring kunt u hier meer over lezen onder het kopje "Direct marketing". Een kopie van onze privacyverklaring treft u in de bijlage aan. Daarnaast kunt deze privacyverklaring op onze website vinden:* www.metaalbedrijfjansen.nl/privacyverklaring. *Graag vernemen wij of u toestemming geeft voor het gebruik van uw persoonsgegevens voor dit doel. U kunt ons uw toestemming geven door hieronder een vinkje te zetten en vervolgens deze offerte ondertekend te retourneren aan ons.* *"□ Ja, ik ga akkoord met verwerking van mijn persoonsgegevens t.b.v. direct marketing zoals is omschreven in uw privacyverklaring."* *Uiteraard kunt u uw toestemming te allen tijde weer intrekken.*	
§ 3.4 (deel 1)	Neem onderaan uw reclamemailings de volgende tekst op en maak gebruik van een afmeldlink om afmelden voor mailings zo eenvoudig mogelijk te maken: *VOORBEELD:* *[NEEMT U HIER DE INHOUD VAN DE MAILING OP]* ***Geen mailings meer ontvangen?*** *U kunt ons te allen tijde kosteloos laten weten dat u geen reclameberichten meer van ons wilt ontvangen. Afmelden voor dit soort berichten kan eenvoudig via de volgende link: [**hyperlink invoegen**].* *Mocht de hyperlink onverhoopt niet werken, neemt u dan contact met ons op: (**naam bedrijf**), (**adres**), (**plaats**), (**e-mail**) en (**telefoonnummer**).*	
§ 3.7 (deel 1)	Als u beheer van (een deel van) uw klant- of leveranciersadministratie uitbesteedt aan een externe partij, persoonsgegevens opslaat op servers van een externe partij of gebruik maakt van een nieuwsbrief mailing dienst van een	

	derde: Sluit met deze partijen een "verwerkersovereenkomst" en gebruik hiervoor de overeenkomst uit bijlage 1. 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 2. Dit is een verplichting van algemene aard die daarom in de volgende delen niet meer aan de orde komt.	
§ 2.1 (alg deel)	Tref passende (organisatorische en technische) maatregelen ter beveiliging van de persoonsgegevens die onderdeel zijn van uw klant- en leveranciersadministratie. U zult dit ook moeten doen voor alle andere persoonsgegevens, bijvoorbeeld die onderdeel uitmaken van de personeels- en loonadministratie, de persoonsgegevens die u d.m.v. uw website verzamelt en alle andere persoonsgegevens die u verwerkt. 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. Omdat dit een algemene verplichting is, komt dit onderwerp in de volgende delen van deze serie niet meer aan de orde.	
Hfd. 7 (alg deel)	Vul het register in dat is opgenomen in bijlage 3. 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. U zult ervoor moeten 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. Ook deze verplichting is van algemene aard en komt daarom in de volgende delen niet meer aan de orde.	
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).	

Bijlagen:

- […] *vul eventueel in*

Hoofdstuk 3: Toelichting op de actiepuntenlijst

§ 3.1 Verwerking persoonsgegevens

Alle bedrijven, dus ook mkb'ers in de metaalbranche, verwerken persoonsgegevens van klanten en leveranciers. Dit kunnen consumenten zijn, maar zijn vaak ook bedrijven of organisaties. Ook als u zakendoet met bedrijven, worden vrijwel altijd persoonsgegevens verwerkt. Bij B2B worden met name persoonsgegevens verwerkt over zelfstandigen en gegevens van contactpersonen die in relatie staan tot een bedrijf of organisatie (meestal medewerkers). Het gaat dan vaak om de volgende categorieën gegevens: naam, adres, plaats, telefoonnummer, e-mailadres en eventueel bankrekeningnummer (bij inkoop, t.b.v. de betaling van facturen).

Bij het verwerken van persoonsgegevens van eenmanszaken en zzp'ers gaat het vaak om zakelijke gegevens die tegelijkertijd privégegevens zijn. Zo kan het vestigingsadres van een ZZP'er tevens zijn woonadres zijn en is zijn mobiele nummer vaak ook zijn telefoonnummer in privé. Bij contactpersonen van bedrijven met wie zaken wordt gedaan gaat het vaak alleen om een naam, (e-mail)adres en eventueel een (rechtstreeks) telefoonnummer.

Levert u zaken of diensten aan consumenten, dan verwerkt u meestal de volgende persoonsgegevens: namen, woonadressen, (privé) telefoonnummers en (privé) e-mailadressen.

Over het algemeen brengt het verwerken van persoonsgegevens van personen in het kader van een relatie of samenwerking met een bedrijf minder risico's met zich mee dan het verwerken van gegevens van personen die deze relatie niet hebben. Dat is ook wel logisch, want bij B2B weet u vaak minder en de informatie waarover u beschikt, is ook minder gevoelig van aard.

Wij gaan er van uit dat u uw klant- en leveranciersgegevens in principe niet aan andere partijen verstrekt, waaronder in ieder geval niet aan partijen in het buitenland of aan internationale organisaties. Dit is namelijk alleen onder voorwaarden toegestaan. Als doorgifte noodzakelijk is in verband met de sluiting of uitvoering van een overeenkomst met de betrokkene, dan is doorgifte toegestaan. Vaak zal doorgifte echter niet 'noodzakelijk' zijn. Wij zullen hier een aantal voorbeelden bij geven:

- Indien u een zonwering voor een consument door een bedrijf in Polen laat vervaardigen, moet u zich afvragen of het verstrekken van de persoonsgegevens van deze klant aan de Poolse partij wel noodzakelijk is. Meestal zal dat niet hoeven en kun u volstaan met doorgifte van de specificaties van het product. Dan is er ook geen sprake van verstrekking van persoonsgegevens. Verstrekt u wel persoonsgegevens, maar is dit niet noodzakelijk voor het sluiten of uitvoeren van de overeenkomst met de klant, dan handelt u in strijd met de AVG.

  Omgekeerd geldt ook dat het veelal niet noodzakelijk zal zijn om persoonsgegevens van de leverancier aan derden, bijvoorbeeld de klant, te verstrekken. Hieronder twee voorbeelden.

- Stel, een klant bestelt bij u een werkboot. Het gewenste model koopt u vervolgens in bij één van uw toeleveranciers om vervolgens aan de klant te leveren. Voor de levering aan de klant is het niet noodzakelijk dat u hem op de hoogte brengt van persoonsgegevens, waaronder contactgegevens, van uw leverancier. Doet u dat wel, dan handelt u in strijd met de AVG.

- Stel, u bent een bedrijf dat zich bezighoudt met het maken van gereedschap. U krijgt de opdracht om volgens tekening van de klant stalen onderdelen te verspanen. Partijen hebben niet afgesproken dat u dit werk per se zelf moet uitvoeren. Wegens drukte besluit u (een deel) van deze opdracht uit te besteden aan een collega-bedrijf. Dit bedrijf levert de onderdelen aan u en u vervolgens aan uw klant. Ook hierbij is het niet noodzakelijk dat u uw klant voorziet van persoonsgegevens van het door u ingeschakelde collega-bedrijf.

In de meeste gevallen zult u met uw klant of leverancier een overeenkomst gaan sluiten tot het leveren van zaken of het verrichten van werkzaamheden. De legitieme reden voor het verzamelen en gebruiken van persoonsgegevens is dan het kunnen uitvoeren van de overeenkomst. Dit is dan

ook meteen uw wettelijke grondslag, op basis waarvan verwerking is toegestaan. Aan de verkoopkant geldt dat als u niet weet wie uw klant is, waar hij woont en hoe u hem kunt bereiken, u uw product ook niet kunt leveren en factureren. Ook aan de inkoopkant heeft u persoonsgegevens nodig: met een rechtspersoon zelf kan je immers niet communiceren, hier zal altijd een 'natuurlijk' persoon aan te pas moeten komen. De persoonsgegevens die u verkrijgt, mag u alleen gebruiken voor uitvoering van de overeenkomst. U hanteert dus het principe "minimale gegevensverwerking", wat inhoudt dat u alleen de voor de uitvoering van de overeenkomst noodzakelijke persoonsgegevens verwerkt. Niet meer en niet minder. Voor de verwerking van de persoonsgegevens hoeft u dan geen toestemming te hebben van de klant.

Wel rust op u een informatieplicht die inhoudt dat u de klant of leverancier moet informeren over de verwerking van persoonsgegevens. Welke informatie u moet verstrekken en wanneer kunt u lezen in paragraaf 3.2 en 3.3.

U mag alleen méér persoonsgegevens verwerken dan die genoemd zijn in het begin van paragraaf 3.1 als dat noodzakelijk is om de overeenkomst met de klant of leverancier uit te kunnen voeren. Wilt u meer gegevens verwerken en is dat niet noodzakelijk, dan heeft u dus een aanvullende grondslag nodig om deze gegevens te mogen verwerken. De ondubbelzinnige toestemming van de klant of de leverancier is dan vaak nog de enige mogelijkheid om dit te mogen doen. U zult dan echter ook voor het deel van de verwerking waar u toestemming voor vraagt aan uw informatieverplichtingen moeten voldoen.

§ 3.2 Informatie die u moet verstrekken

Hieronder zullen wij de informatie opsommen die u aan betrokkenen in zijn algemeenheid moet verstrekken. Daarbij zullen wij uiteraard aangeven hoe bij de onderdelen 'klantbeheer' en 'leveranciersbeheer' concreet invulling kan worden gegeven aan de informatieplicht. In de volgende paragraaf zullen wij aangeven op welke wijze u de informatie aan de betrokkenen kunt verstrekken. Zo mogelijk doen wij ook concrete tekstvoorstellen. Deze tekstvoorstellen zijn ook opgenomen in de actiepuntenlijst voorin dit deel van de serie.

Te verstrekken informatie:

1. U moet de betrokkene informeren over uw identiteit en uw contactgegevens;

   Wij raden aan minimaal 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 zullen geen FG hoeven aan te stellen. Deze informatieverplichting komt daardoor voor hen te vervallen.

3. U moet de betrokkene vertellen waarom u zijn 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 een overeenkomst te sluiten, of de betrokkene verplicht is persoonsgegevens te verstrekken en wat de gevolgen zijn als hij dat niet doet.

   Bij klantbeheer (waarbij u ook aan direct marketing doet) en leveranciersbeheer zou u aan deze informatieverplichting kunnen voldoen door middel van onderstaande tekst:

   > ***Verzamelen en gebruiken van persoonsgegevens van klanten, leveranciers en andere opdrachtnemers***
   > *Graag maken wij u er op attent dat wij de persoonsgegevens die u ons verstrekt zullen verzamelen en gebruiken omdat dit noodzakelijk is om een eventuele overeenkomst met u te sluiten en uit te voeren. Dat geldt zowel voor onze (potentiële) klanten als voor partijen bij wie wij zaken en/of diensten inkopen.*

Bent u een (potentiële) klant van ons, dan gebruiken wij uw gegevens om u een offerte te kunnen toesturen, te kunnen bepalen aan welke specificaties of wensen een bepaalde zaak of dienst dient te voldoen, zaken te kunnen leveren of werkzaamheden voor u te kunnen verrichten, te kunnen factureren en met u vlot en efficiënt te kunnen communiceren over de uitvoeringsaspecten van de overeenkomst.

Bent u een (potentiële) leverancier of andere opdrachtnemer dan zijn uw persoonsgegevens eveneens noodzakelijk voor de sluiting en uitvoering van de overeenkomst. Bij inkoop is dat nodig om u te kunnen laten weten aan welke specificaties of wensen een bepaalde zaak of dienst wat ons betreft dient te voldoen, een offerte-aanvraag te kunnen toesturen of een bestelling bij u te kunnen plaatsen, uw facturen te kunnen betalen en vlot en efficiënt met u te kunnen communiceren over andere aspecten van de overeenkomst.

U bent niet verplicht om ons uw persoonsgegevens te verstrekken. Als u ons geen of onvoldoende persoonsgegevens verstrekt, dan is het echter wel mogelijk dat wij aan de hiervoor genoemde werkzaamheden geen uitvoering kunnen geven.

Direct marketing

OPTIE 1 (als u onderscheid maakt tussen eenmalige klanten en klanten met wie u een duurzame relatie heeft en u alleen de klanten gaat mailen met wie u een duurzame relatie heeft):
Als u regelmatig bij ons bestelt, zullen wij de door u opgegeven persoonsgegevens bewaren en gebruiken om u in de toekomst persoonlijk per e-mail op de hoogte te brengen van onze bestaande en nieuwe producten en diensten en u hier eventueel een aanbieding voor te doen. Wij hebben bij het gebruik van uw persoonsgegevens voor dit doel een gerechtvaardigd belang, namelijk het aan de man brengen van onze producten en diensten. Iedere keer dat wij u een reclamemailing sturen, heeft u de mogelijkheid ons te laten weten hier geen prijs meer op te stellen. Zie hiervoor de afmeldlink onderaan iedere mailing.
Bent u eenmalig klant bij ons, dan zullen wij u alleen reclameberichten toesturen als u ons daar vooraf uw toestemming voor heeft gegeven.

OPTIE 2 (als u géén onderscheid maakt tussen eenmalige klanten en klanten met wie u een duurzame relatie heeft en u daarom al uw klanten om toestemming voor direct marketing vraagt): *Als u ons daarvoor toestemming heeft gegeven, zullen wij de door u opgegeven persoonsgegevens bewaren en gebruiken om u in de toekomst persoonlijk per e-mail op de hoogte te brengen van onze bestaande en nieuwe producten en diensten en u hier eventueel een aanbieding voor te doen. Iedere keer dat wij u een reclamemailing sturen, heeft u de mogelijkheid ons te laten weten hier geen prijs meer op te stellen. Zie hiervoor de afmeldlink onderaan iedere mailing.*

Voor een nadere toelichting op direct marketing verwijzen wij u graag naar § 3.4 van deel 1.

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

   Bij klant- en leveranciersbeheer zal meestal alleen van doorgifte van persoonsgegevens aan een derde sprake zijn als het voor de uitvoering van de overeenkomst met de betrokkene noodzakelijk is persoonsgegevens aan een derde te verstrekken of als verwerkingsactiviteiten worden uitbesteed. 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
   In verband met de uitvoering van een eventuele overeenkomst met u is het mogelijk dat wij uw persoonsgegevens moeten verstrekken aan partijen die onderdelen, materialen en producten aan ons toeleveren of in onze opdracht werkzaamheden uitvoeren. Verder maken wij gebruik van externe serverruimte voor de opslag van (delen van) onze verkoop- en inkoopadministratie, waar uw persoonsgegevens een onderdeel van uitmaken. Uw persoonsgegevens worden om die reden aan onze provider van serverruimte verstrekt.

Verder maken wij gebruik van Microsoft Office en de bijbehorende opslagmogelijkheden voor e-mails en andere bestanden. Omdat wij gebruik maken van een nieuwsbrief mailing dienst, worden uw persoonsgegevens tot slot doorgegeven aan de aanbieder van deze dienst.

5. Als u persoonsgegevens aan partijen/derden doorgeeft die buiten de EER zitten, dan bent u verplicht om de betrokkene 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.

   Bij klant- en leveranciersbeheer: meestal niet van toepassing. Voor zover de doorgifte aan buitenlandse partijen buiten de EER noodzakelijk is voor de uitvoering van de overeenkomst, is doorgifte hoe dan ook toegestaan. Of het land van bestemming adequaat is verklaard of anderszins passende waarborgen biedt, is dan niet meer relevant en hoeft dus ook niet vermeld te worden in de privacyverklaring voor klantbeheer. 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 betrokkene informeren over hoe lang u zijn persoonsgegevens gaat bewaren.

   Bij klantbeheer maken wij een onderscheid tussen personen die uiteindelijk geen klant worden en personen die wel klant zijn geworden. Wij raden u aan om persoonsgegevens van personen die geen klant zijn geworden, bijvoorbeeld omdat zij de offerte van de ondernemer niet gunstig genoeg vonden, tot uiterlijk één jaar na het laatste contact te bewaren. Bij personen die klant worden zou u aansluiting kunnen zoeken bij de duur van de fiscale administratieplicht, die inhoudt dat u uw administratie in veel gevallen zeven jaar moet bewaren ten behoeve van eventuele controles door de Belastingdienst.

   Bij leveranciersbeheer maken wij hetzelfde onderscheid. Besluit u niet in te gaan op de offerte van leverancier, dan adviseren wij u persoonsgegevens van de leverancier binnen een jaar na het laatste contact te verwijderen. Sluit u wel een overeenkomst met de leverancier, dan adviseren wij u wat de termijn van bewaring betreft ook hierbij aansluiting te zoeken bij duur van de fiscale administratieplicht die in veel gevallen zeven jaar zal zijn.

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

   Bewaarperiode persoonsgegevens
   Indien u een offerte bij ons heeft opgevraagd maar u geen klant bij ons geworden bent, zullen wij uw gegevens uiterlijk één jaar na ons laatste contact verwijderen. Ook indien wij een offerte van u hebben ontvangen, maar wij geen klant van u zijn geworden, zullen uw persoonsgegevens uiterlijk één jaar na ons laatste contact worden verwijderd. Bent u wel klant bij ons geworden of wij bij u, dan zullen wij uw persoonsgegevens bewaren voor de duur van zeven jaar na het einde van het boekjaar waarin de overeenkomst met u volledig is uitgevoerd. De periode van zeven jaar komt overeen met de periode waarbinnen wij verplicht zijn onze administratie te bewaren voor de Belastingdienst. Na afloop van deze periode zullen wij uw persoonsgegevens verwijderen.

   Voor een nadere toelichting op de hierboven gekozen bewaartermijn verwijzen wij u graag naar § 3.6 van deel 1.

7. U moet de betrokkene wijzen op de rechten die hij heeft. Het gaat dan om het recht op inzage, rectificatie, wissing, beperking van verwerking, bezwaar, digitale overdracht van zijn gegevens en dat hij het recht heeft een klacht in te dienen bij de AP. Hieronder doen wij een tekstvoorstel voor uw privacyverklaring:

   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 of een klacht indienen bij de Autoriteit Persoonsgegevens. Tot slot kunt u ons verzoeken om verkrijging van uw persoonsgegevens of overdracht van die gegevens aan een ander. 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 betrokkene laten weten dat hij gegeven toestemming voor verwerking van zijn persoonsgegevens ook weer mag intrekken.

   Bij klant- en leveranciersbeheer zal dit meestal niet van toepassing zijn, omdat de grondslag niet "toestemming", maar "uitvoering van de overeenkomst" is. Deze informatieverplichting is alleen van toepassing als u aan direct marketing doet waarvoor u de klant toestemming vraagt. Zie het tekstvoorstel onder punt 3 hierboven.

9. U moet de betrokkene 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 klant- en leveranciersbeheer zal van 'geautomatiseerde individuele besluiten' meestal geen sprake van zijn.

Wij adviseren om met ingang van 25 mei 2018 alle nieuwe klanten en leveranciers 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.

Naar de checklist

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

U moet de informatie uit de vorige paragraaf aan de betrokkenen verstrekken "bij de verkrijging van persoonsgegevens", aldus de AVG. U zult echter niet altijd kunnen informeren voorafgaand aan de verkrijging van persoonsgegevens: soms zal een klant ú immers benaderen en daarbij meteen al persoonsgegevens verstrekken. Logischerwijs kunt u de klant dan pas informeren in uw reactie op het bericht dat deze potentiële klant u heeft gestuurd.

Wij adviseren u aan uw informatieverplichtingen te voldoen door de informatie die u moet verstrekken op te nemen in een zogenaamde "privacyverklaring". Deze privacyverklaring moet u aan uw klanten en leveranciers verstrekken. Bij communicatie per e-mail kunt u de verklaring op uw website zetten, bij schriftelijke communicatie kunt u een exemplaar van de verklaring meesturen.

Plaatst u uw privacyverklaring in ieder geval op een duidelijke en op iedere webpagina zichtbare plaats op uw website. Een goede plek is bijvoorbeeld in de footer van uw website onder de noemer "Privacyverklaring" of "Privacy statement". Door een privacyverklaring op uw website te publiceren, kunnen ook personen die nog geen klant of leverancier zijn alvast informatie vinden over de manier waarop u met hun persoonsgegevens zult omgaan.

U zult bij het eerste (elektronische) contact met uw klant of leverancier het onderwerp privacy al ter sprake moeten brengen. Gebruikt u de gegevens van de klant of leverancier alleen maar om de overeenkomst te sluiten en uit te voeren, dan kunt u de volgende alinea's opnemen in uw bericht aan de klant of leverancier:

> *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. Wij verwijzen u graag naar www.metaalbedrijfjansen.nl/privacyverklaring (hyperlink) voor meer informatie over de verwerking van uw persoonsgegevens en de rechten die u heeft.*

*(**OPTIONEEL: alleen opnemen als u bestaande klanten met wie u een duurzame relatie heeft op basis van een gerechtvaardigd belang mailings gaat versturen over soortgelijke producten of diensten**): Heeft u er bezwaar tegen dat wij uw e-mailadres gaan gebruiken voor het versturen van reclamemailings, laat ons dat dan weten Afmelden voor dit soort berichten kan eenvoudig en kosteloos via de volgende link: [hyperlink invoegen]. Mocht de hyperlink onverhoopt niet werken, neemt u dan contact met ons op via:* info@metaalbedrijfjansen.nl *of op telefoonnummer: 012-345 67 89.*

Voor een nadere toelichting op direct marketing, waar de laatste gecursiveerde alinea hierboven over gaat, verwijzen wij u graag naar § 3.4 van deel 1.

Doet u schriftelijk zaken, dan zal het eerste contact met de klant vaak bestaan uit het afgeven van een offerte. Als u iets wilt inkopen, zal het eerste contact met de leverancier veelal het moment van de offerteaanvraag, of het moment van het plaatsen van de bestelling zijn. Neemt u in het eerste contact met de klant of leverancier, dus in de offerte(-aanvraag) of bestelling, op een duidelijke plaats dan de volgende tekst op:

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 deze privacyverklaring treft u in de bijlage aan. U kunt onze privacyverklaring ook vinden op onze website: www.metaalbedrijfjansen.nl/privacyverklaring *(hyperlink).*

*(**OPTIONEEL: alleen opnemen als u bestaande klanten met wie u een duurzame relatie heeft op basis van een gerechtvaardigd belang mailings gaat versturen over soortgelijke producten of diensten**): Als u klant wordt bij ons zijn we voornemens u reclamemailings te sturen. Zie voor meer informatie hierover onze privacyverklaring. Heeft u bezwaar tegen het gebruik van uw e-mailadres voor reclamemailings, laat ons dat dan weten. Afmelden voor reclamemailings kan eenvoudig en kosteloos via de volgende link: [hyperlink invoegen]. Mocht de hyperlink onverhoopt niet werken, neemt u dan contact met ons op via:* info@metaalbedrijfjansen.nl *of op telefoonnummer: 012-345 67 89.*

Voeg bij uw offerte(-aanvraag)/bestelling ook daadwerkelijk een kopie van uw privacyverklaring en vermeldt het document onder een kopje "Bijlage(n)". Voor een nadere toelichting op direct marketing, waar de laatste gecursiveerde alinea hierboven over gaat, verwijzen wij u graag naar § 3.4 van deel 1.

Wij wijzen u erop dat het onverstandig is de verwijzing naar uw privacyverklaring te 'verstoppen' (bijv. in algemene voorwaarden, of door de verwijzing in een zeer kleine lettergrootte op te stellen, of op een plaats op te nemen die slecht in het oog springt). 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 zijn waarde.

Veel mkb'ers doen nog telefonisch zaken. U zult in dat geval mondeling aan uw informatieplicht moeten voldoen. Concreet betekent dit dat u de klant of leverancier in het eerste telefoongesprek moet vertellen dat u persoonsgegevens gaat verwerken en dat u zich hierbij zult houden aan wat u hierover in uw privacyverklaring heeft opgenomen. U moet tot slot aangeven dat u uw privacyverklaring zult verstrekken. Vervolgens zult u het telefoongesprek moeten laten opvolgen door een brief of een e-mail, waarin u de mondeling gegeven informatie herhaalt en een exemplaar van de privacyverklaring bijvoegt. U kunt daarvoor bovenstaande voorbeeldteksten gebruiken.

Let op, door publicatie van een privacyverklaring op uw website heeft u nog géén toestemming van de betrokkene om zijn persoonsgegevens te verwerken. Hiermee voldoet u alleen aan uw informatieplichten. Verwerkt u persoonsgegevens op basis van toestemming, dan zult u de toestemming nog nadrukkelijk van uw klant moeten verkrijgen.

In bijlage 4 treft u de privacyverklaring voor de klant- en leveranciersadministratie aan. In deze verklaring is dus alle informatie opgenomen waarover u uw klanten en leveranciers moet informeren als u voldoet aan het profiel van metaalbedrijf Jansen. In volgende delen van deze serie zullen wij deze privacyverklaring aanvullen of aanpassen. U heeft immers niet alleen met klanten en leveranciers te maken, maar ook met personeel en eventueel andere personen die van enig

belang zijn voor uw bedrijf. Ieder deel van deze serie zullen wij voorzien van een privacyverklaring die alle informatie bevat die u gelet op de tot dan toe verschenen delen moet verstrekken.

Naar de checklist

§ 3.4 Direct marketing

Veel bedrijven doen aan een vorm van direct marketing. Hieronder verstaan wij het rechtstreeks benaderen van individuele (potentiële) klanten. Ook metaalbedrijf Jansen doet aan direct marketing. Als u de persoonsgegevens niet alleen voor het uitvoeren van een overeenkomst wilt gebruiken, maar ook voor direct marketing, dan gelden aanvullende eisen.

Bij direct marketing heeft u te maken met zowel het spamverbod als de privacyregels. Het spamverbod is geregeld in de Telecommunicatiewet, de privacyregels nu nog in de Wbp en vanaf 25 mei 2017 in de AVG.

Het spamverbod bepaalt dat u alleen commerciële elektronische berichten en nieuwsbrieven aan personen en bedrijven mag versturen als zij daar vooraf duidelijk toestemming voor hebben gegeven. Zijn de personen en bedrijven die u wilt benaderen al klant bij u, dan mag u ze commerciële mailings sturen, mits u de klant bij het verkrijgen van zijn persoonsgegevens duidelijk en uitdrukkelijk de gelegenheid heeft gegeven om kosteloos en eenvoudig te laten weten dat hij geen mailings wil ontvangen. Daarnaast moeten de mailings gaan over producten of diensten die te maken hebben met wat die klanten eerder bij u hebben aangeschaft. In iedere mailing moet u uw identiteit vermelden en een adres, telefoonnummer of e-mailadres opgeven waar de klant zich (wederom eenvoudig en kosteloos) kan afmelden voor verdere mailings. Tot zover de spamregels uit de Telecommunicatiewet. Verder met de regels over direct marketing uit de AVG.

Het na de aankoop van een product of dienst benaderen van klanten om hen andere, nieuwe producten of diensten van u onder de aandacht te brengen, is over het algemeen niet noodzakelijk om de eerdere overeenkomst met de klant uit te kunnen voeren. Van deze grondslag kunt u voor dit type verwerking dan dus geen gebruik maken. Een bedrijf kan echter wel een ‘gerechtvaardigd belang’ hebben bij gebruik van persoonsgegevens voor reclameberichten. Het gaat dan om het commercieel belang bij het aan de man brengen van producten en diensten.

Bij de vraag of direct marketing geoorloofd is, moet een bedrijf een afweging maken tussen het bedrijfsbelang enerzijds en het belang van de betrokkene anderzijds. Weegt het bedrijfsbelang zwaarder dan is direct marketing toegestaan. Uitgangspunt is of de klant redelijkerwijs mag verwachten dat zijn gegevens voor direct marketing worden gebruikt, waarbij de relatie die hij met u heeft een grote rol speelt. De direct marketing moet relevant zijn voor en passen bij de relatie die u met de klant heeft.

Bij incidentele klanten, klanten die eenmalig een aankoop doen en waarbij het niet voor de hand ligt dat zij terugkeren voor een aankoop, raden wij het u vooralsnog af om hun persoonsgegevens te gebruiken voor het toesturen van reclameberichten als zij daar niet vooraf mee hebben ingestemd. De AP zou kunnen vinden dat het gerechtvaardigd belang hier in het gedrang komt, omdat het niet logisch is een incidentele klant reclame te sturen als hij hoogstwaarschijnlijk toch niet tot een nieuwe aankoop overgaat. Wilt u reclame kunnen sturen aan incidentele klanten, dan doet u er verstandig aan om daarvoor vooraf hun ondubbelzinnige toestemming te vragen.

Bij klanten met wie u een duurzame relatie heeft is het sturen van reclameberichten naar onze mening eerder geoorloofd. Een duurzame relatie is een relatie waarbij de klant zich voor een langere tijd heeft verbonden aan uw bedrijf. Dit is wat vaag, maar een voorbeeld is wanneer een klant bij u een onderhoudscontract heeft afgesloten. Waarschijnlijk is ook bij klanten die met enige regelmaat bij u bestellen sprake van een duurzame relatie. Overigens zult u niet altijd meteen weten of een klant een incidentele klant zal zijn of een vaste klant gaat worden. De aard van de producten of diensten die u levert, kunnen een aanwijzing geven. Bij het verkopen van producten aan consumenten door Metaalunieleden denken wij dat dit in de meeste gevallen om eenmalige aankopen zal gaan. Kortom, aan klanten met wie u een duurzame relatie heeft, mag u – zonder toestemming – reclamemailings sturen.

Houdt u zich bij het versturen van reclamemailings verder aan de volgende regels (ongeacht of u toestemming vraagt voor direct marketing):

- U moet de betrokkenen bij het verkrijgen van de persoonsgegevens informeren over uw voornemen hen mailings te sturen en u moet aangeven dat en hoe zij hiertegen bezwaar kunnen maken.
- Gebruik alleen uw eigen klantgegevens voor direct marketing, niet de klantgegevens van een andere partij;
- Beperk het aantal persoonsgegevens dat u voor direct marketing gebruikt (alleen e-mailadressen of NAW-gegevens);
- Pas geen selectie toe (dus stuur al uw klanten dezelfde mailing);
- De mailings hebben betrekking op kwesties die logischerwijs verband houden met de relatie die u heeft met de klant. Kort gezegd zult u uw mailings moeten beperken tot producten en diensten gelijksoortig of aanverwant aan het product of de dienst die de klant in kwestie eerder van u heeft afgenomen. Van belang is het verwachtingspatroon van de klant: ligt de inhoud van uw e-mail in de lijn der verwachting?
- Zorg dat u uw informatieverplichting nakomt;
- In iedere reclamemailing moet u uw identiteit vermelden en opnieuw een (eenvoudige en kosteloze) afmeldmogelijkheid geven.

Onderstaande tekst kunt u aan het slot van uw direct mailings opnemen. Met behulp hiervan biedt u de klant de mogelijkheid zich af te melden, althans zijn bezwaar tegen verdere verwerking kenbaar te maken aan u.

> *VOORBEELD:*
>
> *[NEEMT U HIER DE INHOUD VAN DE MAILING OP]*
>
> ***Geen mailings meer ontvangen?***
> *U kunt ons te allen tijde kosteloos laten weten geen reclameberichten meer te willen ontvangen. Afmelden voor dit soort berichten kan eenvoudig via de volgende link: [**hyperlink invoegen**].*
>
> *Mocht de hyperlink onverhoopt niet werken, neemt u dan contact met ons op: (**naam bedrijf**), (**adres**), (**plaats**), (**e-mail**) en (**telefoonnummer**).*

U kunt er ook voor kiezen om uw klanten niet onder te verdelen in een groep "duurzame klanten" en "incidentele klanten" en ze gemakshalve allemaal om ondubbelzinnige toestemming voor direct marketing te vragen. Dit geeft de meeste zekerheid, maar levert waarschijnlijk wel weinig respons op. Hoe u toestemming voor direct marketing kunt vragen, leest u in de volgende paragraaf.

Naar de checklist

§ 3.5 Toestemming vragen

Als u persoonsgegevens gaat verwerken en u heeft daarvoor toestemming nodig van de betrokkene, bijvoorbeeld in het kader van het sturen van reclameberichten aan eenmalige klanten, dan bepaalt de wet hierover het volgende.

De toestemming moet door middel van een verklaring of een andere ondubbelzinnige actieve handeling worden gegeven. Een betrokkene kan nooit stilzwijgend of op een passieve manier toestemming verlenen. Een actief handelen van zijn kant is noodzakelijk. Werkt u digitaal, dan volstaat een opt-out mogelijkheid niet, opt-in mag wel (het werken met vooraf aangevinkte vakjes is dus geen optie).

De toestemming geldt alleen als deze gebaseerd is op informatie van u over wat u met de gegevens gaat doen in duidelijke en eenvoudige bewoordingen. De informatie moet gemakkelijk toegankelijk zijn. De betrokkene 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 tegelijkertijd informeert. De betrokkene mag op ieder moment zijn toestemming weer intrekken.

Als u eenmalige klanten reclameberichten wilt kunnen sturen, dan heeft u daar ondubbelzinnige toestemming voor nodig. In het eerste bericht dat u aan de klant stuurt, zou u de onderstaande tekstsuggestie kunnen opnemen. De praktijk zal vermoedelijk wel gaan uitwijzen dat op uw verzoek om toestemming te geven nauwelijks respons zal komen. Het versturen van reclameberichten aan eenmalige klanten zal daardoor in de meeste gevallen feitelijk niet mogelijk zijn. Zoals wij al aangaven doet metaalbedrijf Jansen zowel per e-mail als schriftelijk zaken.

Bij zaken doen per e-mail is het advies als volgt:
Neemt u in uw eerste elektronische bericht aan de potentiële klant de volgende tekst op:

> *Wij willen u er in het bijzonder op attent maken dat wij uw persoonsgegevens in de toekomst graag willen gebruiken voor het toesturen van informatie over onze producten en diensten en het eventueel doen van aanbiedingen. In de privacyverklaring op onze website kunt u hier meer over lezen onder het kopje "Direct marketing". Zie hiervoor* www.metaalbedrijfjansen.nl/privacyverklaring*.*
>
> *Graag vernemen wij of u toestemming geeft voor het gebruik van uw persoonsgegevens voor dit doel. U kunt ons uw toestemming geven door een reply te sturen op deze e-mail en in deze reply de volgende zin over te nemen (dat kan eenvoudig met de kopieer- en plakfunctietoetsen):*
>
> > *"Ja, ik ga akkoord met verwerking van mijn persoonsgegevens t.b.v. direct marketing zoals is omschreven in uw privacyverklaring."*
>
> *Uiteraard kunt u uw toestemming te allen tijde weer intrekken.*

Bij schriftelijk zakendoen, is het advies de volgende tekst op te nemen in uw eerste schriftelijke stuk gericht aan de klant (meestal de offerte):

> *Wij willen u er in het bijzonder op attent maken dat wij uw persoonsgegevens in de toekomst graag willen gebruiken voor het toesturen van informatie over onze producten en diensten en het eventueel doen van aanbiedingen. In onze privacyverklaring kunt u hier meer over lezen onder het kopje "Direct marketing". Een kopie van onze privacyverklaring treft u in de bijlage aan. Daarnaast kunt deze privacyverklaring op onze website vinden:* www.metaalbedrijfjansen.nl/privacyverklaring*.*
>
> *Graag vernemen wij of u toestemming geeft voor het gebruik van uw persoonsgegevens voor dit doel. U kunt ons uw toestemming geven door hieronder een vinkje te zetten en vervolgens deze offerte ondertekend te retourneren aan ons.*
>
> > *"☐ Ja, ik ga akkoord met verwerking van mijn persoonsgegevens t.b.v. direct marketing zoals is omschreven in uw privacyverklaring."*
>
> *Uiteraard kunt u uw toestemming te allen tijde weer intrekken.*

Het is onverstandig om in uw offertes op te nemen dat het geven van de opdracht of het plaatsen van de bestelling impliceert dat de klant ook toestemming geeft voor het sturen van reclame. Aan het vereiste van 'ondubbelzinnigheid' is dan hoogstwaarschijnlijk niet voldaan. De AP zal zich waarschijnlijk op het standpunt stellen dat er twijfel kan bestaan over de intentie van de betrokkene. Het instemmen met de offerte hoeft immers niet te betekenen dat de betrokkene ook toestemt met direct marketing.

Wij realiseren ons dat bovenstaande werkwijze in de praktijk niet zal gaan werken. Het is echter de bedoeling van de wetgever geweest om een drempel op te werpen tegen verzending van reclameberichten. Alleen personen die daar écht prijs op stellen, zouden ze moeten ontvangen, de rest moet hiervan gevrijwaard blijven. En dat effect heeft de bovenstaande werkwijze wel.

Naar de checklist

§ 3.6 Bewaartermijn

In de actiepuntenlijst is opgenomen dat u persoonsgegevens die onderdeel uitmaken van uw klant- en leveranciersadministratie maximaal zeven jaar mag bewaren. Volgens de AP is de bewaartermijn bij klanten en leveranciers twee jaar na afhandeling van de transactie of langer als dat noodzakelijk is voor de voldoening aan een wettelijke bewaarplicht. Vanwege dat laatste hebben wij gekozen voor de wettelijke bewaarplicht ten opzichte van de Belastingdienst van zeven jaar. Na die zeven jaar moet u de persoonsgegevens in principe vernietigen.

Wij realiseren ons dat bovenstaande bij u op praktische bezwaren kan stuiten. Bijvoorbeeld omdat u ook na zeven jaar nog geconfronteerd kunt worden met aanspraken van uw klanten, bijvoorbeeld tot reparatie of vervanging van (delen van) uw product. Een ander bezwaar is gelegen in de moeilijkheid om bij te houden wanneer het einde van een bewaartermijn van gegevens wordt genaderd en hoe u de persoonsgegevens dan daadwerkelijk kunt verwijderen.

Wat u zou kunnen doen, is om uw orders (zowel aan de inkoop- als de verkoopkant) een uniek nummer mee te geven dat u ook aan uw klanten en leveranciers verstrekt, zodat u na zeven jaar de persoonsgegevens kunt verwijderen zonder ook meteen alle andere (relevante) informatie van de desbetreffende order te verliezen (productspecificaties, prijzen, technische tekeningen e.d. kunnen dan dus wel bewaard blijven). Laatstgenoemde gegevens, hetgeen geen persoonsgegevens zijn, kunt u dan blijven bewaren.

Voor zover bij ons nu bekend is, biedt de AVG geen ruimte voor een praktischere oplossing ten aanzien van de bewaartermijnen.

Naar de checklist

§ 3.7 Verwerkingsactiviteiten uitbesteden

In het voorgaande zijn we er van uit gegaan dat de mkb'er zelf zijn klant- en leveranciersgegevens bijhoudt, registreert, bewerkt en bewaart. Maar als u het beheer van uw klantgegevens uitbesteedt aan een andere partij, blijft u verantwoordelijk voor deze verwerking. 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 zaken of diensten uitbesteedt die niet of nauwelijks zien op verwerking van persoonsgegevens. Als u een ander bedrijf opdracht geeft tot het vervaardigen en rechtstreeks uitleveren van tien overals voor tien van 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 een bedrijf een ander bedrijf vraagt 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 klant- of leveranciersbeheer 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, de personen wiens gegevens worden verwerkt, 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 bepaald aantal onderwerpen regelt en vastlegt. In de bijlage treft u een voorbeeld overeenkomst hiervoor aan. De geel gearceerde onderdelen zijn de onderwerpen waarvan de AVG voorschrijft dat u ze regelt.

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 gebruik maken 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.

Daarnaast maakt u mogelijk gebruik van een nieuwsbrief mailing dienst (denk bijvoorbeeld aan de online dienst MailChimp). Omdat ook bij partijen die dergelijke diensten aanbieden persoonsgegevens worden opgeslagen, is er sprake een verwerker met wie een verwerkersovereenkomst zou moeten worden gesloten.

Kortom, de meeste mkb'ers zullen in ieder geval verwerkersovereenkomsten moeten sluiten met hun cloudprovider/hostingprovider, het bedrijf dat voor hen (delen van) de klant- en leveranciersadministratie beheert en met de aanbieder van de nieuwsbrief mailing dienst.

Naar de checklist

BIJLAGEN

BIJLAGE 1 : VERWERKERSOVEREENKOMST

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.

Terug naar de checklist

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 2 : VRAGENLIJST T.B.V. DOCUMENTATIE INCIDENTEN

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 3 : REGISTER VOOR VERWERKINGSACTIVITEITEN

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.

BIJLAGE 4 : PRIVACYVERKLARING (BIJGEWERKT TOT EN MET DEEL 1)

PRIVACYVERKLARING

Verzamelen en gebruiken van persoonsgegevens van klanten, leveranciers en andere opdrachtnemers
Graag maken wij u er op attent dat wij de persoonsgegevens die u ons verstrekt zullen verzamelen en gebruiken omdat dit noodzakelijk is om een eventuele overeenkomst met u te sluiten en uit te voeren. Dat geldt zowel voor onze (potentiële) klanten als voor partijen bij wie wij zaken en/of diensten inkopen.

Bent u een (potentiële) klant van ons, dan gebruiken wij uw gegevens om u een offerte te kunnen toesturen, te kunnen bepalen aan welke specificaties of wensen een bepaalde zaak of dienst dient te voldoen, zaken te kunnen leveren of werkzaamheden voor u te kunnen verrichten, te kunnen factureren en met u vlot en efficiënt te kunnen communiceren over de uitvoeringsaspecten van de overeenkomst.

Bent u een (potentiële) leverancier of andere opdrachtnemer dan zijn uw persoonsgegevens eveneens noodzakelijk voor de sluiting en uitvoering van de overeenkomst. Bij inkoop is dat nodig om u te kunnen laten weten aan welke specificaties of wensen een bepaalde zaak of dienst wat ons betreft dient te voldoen, een offerte-aanvraag te kunnen toesturen of een bestelling bij u te kunnen plaatsen, uw facturen te kunnen betalen en vlot en efficiënt met u te kunnen communiceren over andere aspecten van de overeenkomst.

U bent niet verplicht om ons uw persoonsgegevens te verstrekken. Als u ons geen of onvoldoende persoonsgegevens verstrekt, dan is het echter wel mogelijk dat wij aan de hiervoor genoemde werkzaamheden geen uitvoering kunnen geven.

Doorgifte aan derden
In verband met de uitvoering van een eventuele overeenkomst met u is het mogelijk dat wij uw persoonsgegevens moeten verstrekken aan partijen die onderdelen, materialen en producten aan ons toeleveren of in onze opdracht werkzaamheden uitvoeren. Verder maken wij gebruik van externe serverruimte voor de opslag van (delen van) onze verkoop- en inkoopadministratie, waar uw persoonsgegevens een onderdeel van uitmaken. Uw persoonsgegevens worden om die reden aan onze provider van serverruimte verstrekt. Omdat wij gebruik maken van een nieuwsbrief mailing dienst, worden uw persoonsgegevens tot slot doorgegeven aan de aanbieder van deze dienst.

Direct marketing

OPTIE 1 (als u onderscheid maakt tussen eenmalige klanten en klanten met wie u een duurzame relatie heeft en u alleen de klanten gaat mailen met wie u een duurzame relatie heeft):
Als u regelmatig bij ons bestelt, zullen wij de door u opgegeven persoonsgegevens bewaren en gebruiken om u in de toekomst persoonlijk per e-mail op de hoogte te brengen van onze bestaande en nieuwe producten en diensten en u hier eventueel een aanbieding voor te doen. Wij hebben bij het gebruik van uw persoonsgegevens voor dit doel een gerechtvaardigd belang, namelijk het aan de man brengen van onze producten en diensten. Iedere keer dat wij u een reclamemailing sturen, heeft u de mogelijkheid ons te laten weten hier geen prijs meer op te stellen. Zie hiervoor de afmeldlink onderaan iedere mailing.
Bent u eenmalig klant bij ons, dan zullen wij u alleen reclameberichten toesturen als u ons daar vooraf uw toestemming voor heeft gegeven.

OPTIE 2 (als u géén onderscheid maakt tussen eenmalige klanten en klanten met wie u een duurzame relatie heeft en u daarom al uw klanten om toestemming voor direct marketing vraagt): *Als u ons daarvoor toestemming heeft gegeven, zullen wij de door u opgegeven persoonsgegevens bewaren en gebruiken om u in de toekomst persoonlijk per e-mail op de hoogte te brengen van onze bestaande en nieuwe producten en diensten en u hier eventueel een aanbieding voor te doen. Iedere keer dat wij u een reclamemailing sturen, heeft u de mogelijkheid ons te laten weten hier geen prijs meer op te stellen. Zie hiervoor de afmeldlink onderaan iedere mailing.*

Bewaarperiode persoonsgegevens
Indien u een offerte bij ons heeft opgevraagd maar u geen klant bij ons geworden bent, zullen wij uw gegevens uiterlijk één jaar na ons laatste contact verwijderen. Ook indien wij een offerte van u hebben ontvangen, maar wij geen klant van u zijn geworden, zullen uw persoonsgegevens uiterlijk één jaar na ons laatste contact worden verwijderd. Bent u wel klant bij ons geworden of wij bij u, dan zullen wij uw persoonsgegevens bewaren voor de duur van zeven jaar na het einde van het boekjaar waarin de overeenkomst met u volledig is uitgevoerd. De periode van zeven jaar komt overeen met de periode waarbinnen wij verplicht zijn onze administratie te bewaren voor de Belastingdienst. Na afloop van deze periode zullen wij uw persoonsgegevens verwijderen.

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 of een klacht indienen bij de Autoriteit Persoonsgegevens. Tot slot kunt u ons verzoeken om verkrijging van uw persoonsgegevens of overdracht van die gegevens aan een ander. 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.*

*[**datum invullen waarop u de privacyverklaring heeft gepubliceerd**]*