# HANDREIKING PERSOONSGEGEVENS BIJ BOUW, RENOVATIE EN ONDERHOUD

vereniging van woningcorporaties

aedes

Bouwend Nederland

de vereniging van bouw- en infrabedrijven

UNETO-VNI

PRIVACY COMPANY

# INHOUD

# PRIVACY IN HET ALGEMEEN

**Steeds meer gegevens zijn digitaal beschikbaar. Informatie over vastgoed, maar ook over mensen en hun gedrag. Als organisatie of ondernemer zal u ongetwijfeld ook te maken krijgen met gegevens over personen, of dit nu adresgegevens zijn of meer persoonlijke informatie. Het zal u niet verbazen dat het gebruik van deze gegevens aan strikte wettelijke regels is gebonden. Een belangrijke regel die in 2016 in werking is getreden is de meldplicht datalekken: organisaties die een datalek constateren moeten dat melden aan de Autoriteit Persoonsgegevens en soms ook bij de personen op wie de gegevens betrekking hebben. Datalekken kunnen grote gevolgen hebben. Met een kopie van een paspoort bijvoorbeeld kunnen criminelen leningen afsluiten of een ruimte voor een wietplantage huren. Per dag zijn er in Nederland zo'n 500 gevallen van identiteitsfraude bekend. Daarnaast krijgt u per 25 mei 2018 te maken met strengere privacyregels, omdat dan de Europese Algemene Verordening Gegevensbescherming in werking treedt. Hierbij valt te denken aan regels voor het verstrekken van gegevens aan andere partijen, het bijhouden van zwarte lijsten, het aanstellen van een functionaris voor de Gegevensbescherming en nog heel veel andere aspecten. Handelt u in strijd met de wet, dan loopt u het risico op een boete die kan oplopen tot duizenden euro's.**

# OVER VERANTWOORDELIJKEN EN BEWERKERS

Als opdrachtgever of opdrachtnemer (woningcorporatie, aannemer of installateur) heeft u veel te maken met het uitwisselen van persoonsgegevens. Hierbij kan gedacht worden aan het uitwisselen van adresgegevens tussen een woningcorporatie en aannemer of installateur, het verstrekken van gegevens aan een opdrachtgever, maar ook aan het rapporteren van overlast door een bewoner bij de gemeente of politie.
Al deze uitwisselingen van persoonsgegevens zijn echter aan regels gebonden. In Nederland zijn deze regels op dit moment nog opgenomen in de Wet bescherming persoonsgegevens (hierna: Wbp), maar op 25 mei 2018 gaat dit veranderen. Op die dag wordt namelijk de Algemene Verordening Gegevensbescherming (hierna: AVG) van kracht, waarmee het privacyrecht binnen de gehele Europese Unie in één keer op een gelijk niveau wordt getrokken.

In de Wbp staan twee partijen centraal als het gaat om de uitwisseling van persoonsgegevens: de *verantwoordelijke* en de *bewerker*. In de aankomende Algemene Verordening Gegevensbescherming (hierna: AVG) is deze terminologie iets veranderd. In de AVG wordt niet langer gesproken over verantwoordelijke en bewerker maar over *verwerkingsverantwoordelijke* en *verwerker.* Het gaat echter nog steeds over dezelfde partijen. Wel veranderen de verantwoordelijkheden die op beiden rusten.

Welke verantwoordelijkheden dit precies zijn is in de praktijk nog lang niet altijd goed afgebakend, noch is in veel gevallen duidelijk welke partij welke rol vervult. Dit is de reden geweest voor het opstellen van deze handreiking. Aan de hand van de Wbp en de AVG zal u een duidelijk en praktisch overzicht worden geboden van de rolverdeling tussen de verantwoordelijke en de bewerker en de verantwoordelijkheden die bij deze rollen komen kijken. Hierbij zal in principe nog worden uitgegaan van de Wbp, maar waar dit nodig is zal worden aangegeven welke veranderingen er onder de AVG zullen plaatsvinden. Dit overzicht kan dienen als basis en leidraad voor onderhandelingen en het goed inrichten van gegevensuitwisselingen. De handreiking zal hierbij gebruikmaken van praktijksituaties om de behandelde materie concreet te maken. Daarnaast zijn aan het eind van de handreiking een model bewerkersovereenkomst, een modelregeling gezamenlijke verantwoordelijkheid, modelbepalingen privacy ten behoeve van algemene voorwaarden en een lijst met praktische vragen en antwoorden opgenomen. Deze praktische vragen en antwoorden zullen gedeeltelijk aansluiten bij de praktijksituaties die eerder aan bod zijn gekomen.

# WAT ZIJN PERSOONSGEGEVENS EN WAT MOET MIJN ORGANISATIE HIER VOOR REGELEN?

## PERSOONSGEGEVENS

Wat zijn persoonsgegevens? Om iets over de uitwisseling van persoonsgegevens te kunnen zeggen moet eerst duidelijk zijn wat dan precies persoonsgegevens zijn. Kortgezegd zijn persoonsgegevens alle gegevens die mogelijkerwijs iets kunnen zeggen over een bepaald persoon. Dit betreft dus een hele brede categorie van gegevens. In de Wet bescherming persoonsgegevens staat in artikel 1 sub a het volgende: *'persoonsgegeven': elk gegeven betreffende een geïdentificeerde of identificeerbare persoon.*

**VOORBEELD**

EEN WONINGCORPORATIE, AANNEMER OF INSTALLATEUR KAN DE BESCHIKKING HEBBEN OVER ADRESGEGEVENS VAN KLANTEN, BIJVOORBEELD OMDAT BIJ DEZE KLANTEN ONDERHOUD IS VERRICHT. DOORDAT DEZE ADRESGEGEVENS GEMAKKELIJK AAN EEN NAAM KUNNEN WORDEN GEKOPPELD EN DAARMEE IETS ZEGGEN OVER DE PERSOON DIE OP HET BETREFFENDE ADRES WOONT (NAMELIJK WAAR DEZE PERSOON WOONT) ZIJN DIT PERSOONSGEGEVENS. OOK BIJVOORBEELD EMAIL ADRESSEN EN TELEFOONNUMMERS ZIJN HIERDOOR PERSOONSGEGEVENS.
**NB:** DIT GELDT VOOR ZOWEL GEGEVENS OP PAPIER ALS DIGITAAL.

## VERWERKING VAN PERSOONSGEGEVENS

Voordat een persoon of organisatie de rol van verantwoordelijke/bewerker kan innemen, moet allereerst sprake zijn van een verwerking van persoonsgegevens. De verantwoordelijkheden binnen de rollen van verantwoordelijke en bewerker zijn namelijk bedoeld om deze verwerkingen zo goed en veilig mogelijk te laten verlopen.

De definitie van verwerking van persoonsgegevens is te vinden in artikel 1 sub b van de Wbp en artikel 4 lid 2 van de AVG. In de Wbp staat onder *'verwerking van persoonsgegevens': elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van persoonsgegevens.*

De bovenstaande lijst is niet bedoeld als een volledige opsomming, wat er op neer komt dat in principe alles wat met een persoonsgegeven gebeurt als verwerking kan worden aangemerkt. De AVG schaart ook het *structureren* van persoonsgegevens onder verwerkingen en voegt nog toe dat ook een *geautomatiseerd proces* onder verwerken valt.

Belangrijk hier is dat het dus niet vereist is dat u een persoonsgegeven aanpast of verandert. Alleen het bijhouden van een database van of inzien van persoonsgegevens is al voldoende om van een verwerking te spreken.

**VOORBEELD**

EEN WONINGCORPORATIE *DRAAGT DE ADRESGEGEVENS VAN HAAR HUURDERS* OVER AAN EEN AANNEMER/INSTALLATEUR, ZODAT DEZE ONDERHOUD/INSTALLATIEWERKZAAMHEDEN KAN VERRICHTEN AAN DE BETREFFENDE WONINGEN. DEZE OVERDRACHT VAN PERSOONSGEGEVENS IS EEN *VERWERKING*. ALS DE AANNEMER/INSTALLATEUR DEZE GEGEVENS VERVOLGENS *GEBRUIKT OM DE JUISTE HUURWONING TE VINDEN* IS ER *WEER* SPRAKE VAN EEN *VERWERKING*.

## VERANTWOORDELIJKE (AVG: VERWERKINGSVERANTWOORDELIJKE)

Op het moment dat persoonsgegevens worden verwerkt moet iemand voor dit gebruik aansprakelijk zijn. Anders kan een betrokkene (de persoon op wie de persoonsgegevens van toepassing zijn) nooit weten wie hij moet aanspreken als er een fout wordt gemaakt met de persoonsgegevens. Deze aansprakelijke persoon of organisatie wordt door de Wbp toepasselijk aangemerkt als 'verantwoordelijke'. Onder de AVG wordt dit, zoals gezegd, de 'verwerkingsverantwoordelijke'. De definitie van verantwoordelijke is terug te vinden in artikel 1 sub d van de Wbp en artikel 4 lid 7 van de AVG. In de Wbp staat het volgende:

*d. verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;*

Er zijn drie elementen in deze definitie te onderscheiden, te weten:

1. natuurlijk persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat
2. alleen of tezamen met anderen
3. het doel van en de middelen voor de verwerking persoonsgegevens vaststelt.

Deze afzonderlijke elementen zullen hieronder één voor één worden toegelicht.

### Natuurlijk persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat

De rol van verantwoordelijke voor een verwerking kan op een aantal verschillende manieren worden ingevuld. De verantwoordelijke kan een natuurlijk persoon zijn (jij of ik), een rechtspersoon (een bv, nv, vereniging, et cetera) of een bestuursorgaan (bijvoorbeeld een gemeente of de overheid).
Daarnaast is er de categorie 'ieder ander'. Dit kan gezien worden als een restcategorie en illustreert het feit dat de rol van verantwoordelijke niet gebonden is aan vooropgestelde rechtsvormen, maar bepaald wordt door de feitelijke gang van zaken binnen organisaties. Er wordt dus gekeken hoe een gegevensuitwisseling in de praktijk is vormgegeven; wie welke gegevens precies uitwisselt met wie en op welke manier.

**VOORBEELD**

ZOWEL EEN WONINGCORPORATIE ALS EEN AANNEMER ALS EEN INSTALLATEUR KAN VERANTWOORDELIJKE ZIJN ALS HET GAAT OM PERSOONSGEGEVENS. VERANTWOORDELIJKHEID IS NIET GEBONDEN AAN EEN BEPAALDE RECHTSVORM.

### Alleen of tezamen met anderen

Het zal vaak zo zijn dat er maar één verantwoordelijke is per verwerking. Het is echter ook mogelijk dat het doel en de middelen van de verwerking (zie hieronder) door meerdere personen/organisaties samen bepaald worden. In dat geval is er sprake van meerdere verantwoordelijken voor één verwerking, ook wel *medeverantwoordelijkheid* genoemd. De details van deze constructie zullen verderop in deze handreiking nog apart worden besproken.

### Het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt

Dit is het belangrijkste element bij het bepalen wie de rol van verantwoordelijke vervult. De wet heeft hiermee een duidelijk onderscheid willen aanbrengen tussen de verantwoordelijke en de *bewerker*. Het is namelijk de verantwoordelijke, en niet de bewerker, die volgens de Wbp het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Anders gezegd beantwoordt de verantwoordelijke de volgende vragen:

1. Waarom/Met welk doel gaan we persoonsgegevens verwerken?
2. Hoe/Met welke middelen gaan we deze persoonsgegevens verwerken?

De verantwoordelijke is dus de persoon of organisatie die het initiatief neemt om persoonsgegevens te gaan verwerken (de waarom-vraag), die vervolgens bepaalt welke persoonsgegevens gebruikt zullen worden en op wat voor manier die persoonsgegevens worden gebruikt (de hoe-vraag). Hierbij is het van belang te weten dat het 'doel' van de verwerking zo specifiek mogelijk geformuleerd moet worden, maar dat de reikwijdte in de praktijk heel ruim kan zijn. Hierbij kan bijvoorbeeld gedacht worden aan: 'het verrichten van onderhoudswerkzaamheden bij klanten' of 'HRM-zaken'.

Naast het *doel* van de verwerking stelt de verantwoordelijke zoals gezegd ook de *middelen* voor het verwerken van de persoonsgegevens vast. Hierbij kan het zowel om *technische middelen* gaan – bijvoorbeeld software of hardware waar de persoonsgegevens op staan – maar ook om *organisatorische middelen*; bedrijfsprocessen of beveiligingsmaatregelen. De verantwoordelijke hoeft voor de vaststelling hiervan niet elk detail van de verwerkingsmiddelen te kennen. Het kan immers zo zijn dat een bewerker juist om zijn technische expertise wordt ingeschakeld, de bewerker is dan in feite zelf het middel. Daarom dient de verantwoordelijke slechts de hoofdlijnen van de verwerkingsmiddelen te bepalen en mag hij de nadere invulling daarvan overlaten aan de bewerker. Er moet echter altijd sprake zijn van een ondergeschikte relatie. Relaties binnen een organisatie vallen daar echter buiten, dus een medewerker is geen bewerker als zijn baas de verantwoordelijke is. Het betreft dan dezelfde organisatie en de medewerker handelt als verantwoordelijke. Als de bewerker *volledige zeggenschap* heeft over het gebruik van de middelen is echter niet langer sprake van een verantwoordelijke-bewerkerrelatie maar van medeverantwoordelijkheid.

**VOORBEELD**
HET DOEL VAN *HET VERRICHTEN VAN ONDERHOUD BIJ EEN KLANT (DE WAAROM-VRAAG)* VAN EEN WONINGCORPORATIE, WORDT DOOR DE WONINGCORPORATIE BEREIKT DOOR *HET VERSTREKKEN VAN GEGEVENS VAN DE BETREFFENDE HUURDERS AAN EEN AANNEMER/ INSTALLATEUR (DE HOE-VRAAG).*

### WAT IS BELANGRIJK BIJ HET VASTSTELLEN VAN WIE DE VERANTWOORDELIJKE IS?

Bij het vaststellen wie de verantwoordelijke is en wie bewerker moet in het oog gehouden worden dat de rol van verantwoordelijke bovenal functioneel wordt ingevuld. Dit betekent dat de verantwoordelijkheid komt te liggen bij de partij(en) waar de daadwerkelijke bepaling van het doel en de middelen plaatsvindt. U kunt hier dus met name door middel van de praktische uitvoering invloed op uitoefenen.

Een afgesloten bewerkersovereenkomst is geen bepalende factor als het gaat om het aanwijzen van een verantwoordelijke of bewerker. Een persoon of organisatie kan in een bewerkersovereenkomst als verantwoordelijke worden aangemerkt, maar als dit niet tot uiting komt doordat deze persoon of organisatie het doel en de middelen van de verwerking vaststelt zal in plaats daarvan de persoon of de organisatie die dit wél doet worden aangemerkt als verantwoordelijke. Dit betekent dat verwerkingen door natuurlijke personen binnen een rechtspersoon zullen worden toegerekend aan de rechtspersoon en dat verwerkingen binnen een eenmanszaak worden toegerekend aan de natuurlijke persoon. Daarnaast is het mogelijk dat een verantwoordelijke door de wet wordt aangewezen (formeel verantwoordelijke). Een voorbeeld hiervan is de belastingdienst. Formele verantwoordelijkheid is echter niet van toepassing bij woningcorporaties, aannemers of installateurs.

### MEDEVERANTWOORDELIJKHEID

Het is mogelijk dat er in de relatie tussen twee partijen geen sprake is van een verantwoordelijke en een bewerker, maar van twee verantwoordelijken. Dit is onder andere mogelijk doordat het doel en de middelen door meerdere personen/organisaties bepaald kunnen worden. In dat geval is er sprake van meerdere verantwoordelijken voor één verwerking ook wel *medeverantwoordelijkheid* genoemd. Daarnaast is het mogelijk dat een bewerker de persoonsgegevens ook voor een eigen doel verwerkt. Voor de verwerkingen die in het kader van dat andere doel worden uitgevoerd is de bewerker dan verantwoordelijke, met alle verantwoordelijkheden en aansprakelijkheden die daar bij komen kijken (zie de volgende paragraaf). Ook hier is een bewerkersovereenkomst niet leidend. Het kan zo zijn dat er een bewerkersovereenkomst is afgesloten tussen een verantwoordelijke en een beoogd bewerker, maar dat door de feitelijke invloed die de bewerker heeft op de bepaling van het doel of de middelen sprake is van medeverantwoordelijkheid (de bewerker is dan dus geen bewerker maar de feitelijke verantwoordelijke).

Medeverantwoordelijken zijn onder de AVG verplicht om hun wederzijdse verplichtingen vast te leggen in een regeling. Deze regeling kan verschillende vormen aannemen. Hierbij kan gekozen worden voor het opnemen van bepalingen met betrekking tot de verwerking van persoonsgegevens in de algemene

voorwaarden, de overeenkomst van opdracht of de inkoopvoorwaarden, of er kan een aparte regeling gezamenlijke verantwoordelijkheid worden overeengekomen. Deze laatste is enigszins vergelijkbaar met een bewerkersovereenkomst en biedt meer mogelijkheden om in te spelen op de specifieke omstandigheden van de verwerking.

Bij het vastleggen van de verplichtingen is het met name van belang dat betrokkenen hun rechten op een goede manier kunnen uitoefenen. In principe is het bij medeverantwoordelijkheid namelijk zo dat de betrokkenen op wie de persoonsgegevens betrekking hebben bij iedere verantwoordelijke terecht moeten kunnen om hun rechten uit te oefenen. Wie de verantwoordelijke is die uiteindelijk uitvoering moet geven aan (bijvoorbeeld) een beroep op inzage kan worden vastgelegd in de voornoemde standaardbepalingen of regeling. In beide gevallen moet duidelijk blijken wat de onderlinge verhouding tussen de verantwoordelijken is (artikel 26 AVG).

Aan het eind van deze handreiking zijn een modelregeling gezamenlijke verantwoordelijkheid en standaardbepalingen met betrekking tot de verwerking van persoonsgegevens opgenomen. Als voor de modelregeling wordt gekozen moet deze nog wel worden aangevuld met de specifieke omstandigheden van de verwerking waar deze op van toepassing is. Dit biedt een goed uitgangspunt bij het vaststellen van de wederzijdse verantwoordelijkheden in geval van medeverantwoordelijkheid.

**VOORBEELD**

EEN WONINGCORPORATIE WERKT SAMEN MET EEN AANNEMER/INSTALLATEUR OM ONDERHOUD/INSTALLATIEWERKZAAMHEDEN TE VERRICHTEN BIJ KLANTEN. DE WONINGCORPORATIE IS VERANTWOORDELIJKE VOOR DE PERSOONSGEGEVENS DIE ZIJ ONDER ZICH HEEFT. DE AANNEMER/INSTALLATEUR IS GEEN BEWERKER OMDAT HIJ NIET PRIMAIR WORDT INGESCHAKELD OM DE PERSOONSGEGEVENS TE GEBRUIKEN, MAAR OM ONDERHOUD/INSTALLATIEWERKZAAMHEDEN UIT TE VOEREN. HIJ VERWERKT ECHTER WEL DE PERSOONSGEGEVENS OM DE JUISTE ADRESSEN TE KUNNEN VINDEN. HIERDOOR IS ER SPRAKE VAN MEDEVERANTWOORDELIJKHEID.

## VERANTWOORDELIJKHEDEN VAN DE VERANTWOORDELIJKE

Het is van belang om vast te stellen wie de verantwoordelijke voor een verwerking is, aangezien de verantwoordelijke degene is die moet zorgen dat de verwerking in overeenstemming met de Wbp/AVG wordt uitgevoerd (artikel 15 Wbp). Op het moment dat een verwerking niet in overeenstemming met de Wbp/AVG plaatsvindt is de verantwoordelijke in ieder geval aansprakelijk en loopt deze het risico op aanzienlijke boetes. Het is daarom van groot belang dat een verantwoordelijke zich goed bewust is van zijn verantwoordelijkheden.

De verantwoordelijkheden van de verantwoordelijke worden op verscheidene plaatsen in de wet beschreven. Deze zullen hier kort worden opgesomd. Voor een uitgebreidere beschrijving kan de *Handreiking gegevensbescherming* worden geraadpleegd.[1]

De verantwoordelijke draagt er zorg voor dat:

- Persoonsgegevens op een zorgvuldige en behoorlijke wijze worden verwerkt, in overeenstemming met de wet (artikel 6 Wbp).
- De verwerking plaatsvindt met een rechtmatige grondslag (artikel 8 Wbp).
- Verdere verwerking van persoonsgegevens slechts plaatsvindt op grond van welbepaalde, uitdrukkelijk omschreven, gerechtvaardigde doelen (artikel 7, 9 en 43 Wbp).
- Persoonsgegevens alleen worden verwerkt indien de kwaliteit op orde is, de gegevens ter zake dienen en niet bovenmatig worden verwerkt (artikel 11 Wbp).
- Verwerkingen van persoonsgegevens worden gemeld bij de AP (artikel 27 Wbp). *Deze verantwoordelijkheid vervalt onder de AVG.*

1 *Handreiking gegevensbescherming*, Aedes 2016, Hfst 1 t/m 13

- Er passende technische en organisatorische beveiligingsmaatregelen worden genomen om de persoonsgegevens te beschermen (artikel 13 Wbp). *Indien de verwerkingsactiviteiten hiertoe aanleiding geven (bijvoorbeeld door schaal of door de gevoeligheid van gegevens) moet de verantwoordelijke onder de AVG een beveiligingsbeleid hebben (artikel 24 lid 2 AVG).*
- Waar nodig moeten afspraken met derden worden gemaakt over de verwerking van persoonsgegevens (artikel 14 Wbp).
- Persoonsgegevens niet nodeloos (lang) worden bewaard (artikel 10 Wbp).
- Een functionaris voor de gegevensbescherming wordt ingesteld (FG) (artikel 62-64 Wbp).
- De betrokkene een beroep kan doen op zijn recht op informatie over de verwerking van zijn persoonsgegevens (artikel 33 en 34 Wbp).
- De betrokkene een beroep kan doen op zijn recht op inzage, wijziging, verwijdering van de eigen persoonsgegevens (artikel 35, 36, 40-41 Wbp) en het recht om niet te worden onderworpen aan geautomatiseerde individuele besluitvorming (artikel 42 Wbp). *Onder de AVG komen hier nog het recht op beperking van de verwerking (artikel 18 AVG) en het recht op overdraagbaarheid van gegevens (artikel 20 AVG) bij.*
- Voldaan wordt aan de aparte, strengere regimes voor de verwerking van bijzondere persoonsgegevens (artikel 16-23 Wbp) en gevoelige persoonsgegevens, waaronder wettelijke persoonsnummers (artikel 24 Wbp).
- Datalekken bij de AP en aan betrokkene worden gemeld (artikel 34a Wbp).

Daarnaast krijgt de verantwoordelijke er als verwerkingsverantwoordelijke onder de AVG nog een aantal extra verantwoordelijkheden bij:

- De verwerkingsverantwoordelijke moet bij het ontwikkelen van (nieuwe) producten of diensten rekening houden met privacy by design en privacy by default.
- De verwerkingsverantwoordelijke moet er voor zorgen dat hij alleen een beroep doet op verwerkers (bewerkers) die afdoende garanties bieden met betrekking tot de passende technische en organisatorische beveiligingsmaatregelen om de persoonsgegevens te beschermen, die persoonsgegevens conform de AVG verwerken en die de rechten van betrokkenen voldoende waarborgen. Het gaat dan onder andere om het recht van inzage, wijziging en verwijdering van eigen persoonsgegevens (artikel 28 AVG).
- De verwerkingsverantwoordelijke moet een register bijhouden van alle verwerkingsactiviteiten met betrekking tot persoonsgegevens (artikel 30 AVG).
- De verwerkingsverantwoordelijke moet bij risicovolle verwerkingen, van tevoren, een Privacy Impact Assessment (PIA) uitvoeren (artikel 35 AVG). Of een verwerking risicovol is wordt bepaald aan de hand van de aard, de omvang, de context en de doeleinden van de verwerking.

# BEN IK/IS MIJN ORGANISATIE VERANTWOORDELIJKE?

Als u de volgende vragen met 'ja' kunt beantwoorden bent u zeer waarschijnlijk de verantwoordelijke:

- Bepaalt u welke persoonsgegevens u nodig heeft voor de uitvoering van uw werk?
- Bepaalt u het doel van de verwerking? (Wat gaan we doen?)
- Bepaalt u in hoofdlijnen de middelen die gebruikt worden voor de verwerking (technisch en organisatorisch)? (Hoe gaan we dat doen?)
  - Heeft u in dit kader een bewerker primair ingeschakeld wegens zijn/haar expertise en bepaalt de bewerker daarom de *nadere* uitwerking van de gebruikte middelen?[2]
- Bepaalt u de bewaartermijn/bepaalt u wanneer de persoonsgegevens gewist moeten worden?
- Bepaalt u de mate en wijze van beveiliging van de persoonsgegevens?
- Bepaalt u wie er toegang hebben tot de persoonsgegevens?

Indien u bij bepaalde vragen 'nee' heeft geantwoord, bent u voor dit gedeelte wellicht niet de verantwoordelijke. In dat geval kan er sprake zijn van medeverantwoordelijkheid. Indien u geen van de vragen met 'ja' kon beantwoorden, bent u waarschijnlijk een bewerker. In het volgende onderdeel worden de verantwoordelijkheden van de bewerker uiteengezet.

2 Pas op! In dit specifieke geval moet er goed worden gekeken naar hoeveelheid invloed die de verantwoordelijke heeft op het bepalen van de middelen. Als de verantwoordelijke niets meer te zeggen heeft over de middelen, is hij voor dit deel niet langer verantwoordelijke, maar wordt de bewerker die de middelen bepaalt voor dit deel de verantwoordelijke (medeverantwoordelijkheid).

# BEWERKER (AVG: VERWERKER)

De term *bewerker* is enigszins misleidend. Dit lijkt te impliceren dat, voordat men wordt aangemerkt als bewerker, sprake moet zijn van een 'bewerking' van persoonsgegevens, oftewel een actieve aanpassing/verandering van de persoonsgegevens. Dit is echter niet het geval. Een aanpassing van de persoonsgegevens is niet vereist om als bewerker aangemerkt te worden. Deze onduidelijkheid wordt enigszins verholpen met de inwerkingtreding van de AVG. Onder de AVG wordt de term 'bewerker' namelijk verandert in 'verwerker'.

De definitie van bewerker is te vinden in artikel 1 sub e van de Wbp en artikel 4 lid 8 van de AVG. De Wbp stelt in artikel 1 sub e:

e. *bewerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen*

In deze definitie zijn twee elementen te onderscheiden:

**Ten behoeve van de verantwoordelijke**

Dit betekent dat een bewerker geen persoonsgegevens voor zichzelf mag verwerken. De bewerker mag geen initiatief tot het verwerken van persoonsgegevens nemen, dit initiatief moet van de verantwoordelijke afkomstig zijn. Er wordt in deze context wel gesproken over het 'slaafs volgen' van de instructies van de verantwoordelijke. Daarnaast bestaan de hoofdwerkzaamheden van de bewerker uit het verwerken van persoonsgegevens voor de verantwoordelijke. De bewerker bepaalt dan ook niet wat het doel van de verwerking is en mag ook geen ander eigen doel behartigen met het verwerken van de persoonsgegevens. De verwerking van persoonsgegevens mag geen bijkomstigheid zijn bij het uitvoeren van de hoofdwerkzaamheden. Is dit wel het geval dan is hij voor dit deel *zelf de verantwoordelijke*. Dit betekent dat hij ook als verantwoordelijke kan worden aangesproken voor deze verwerking en dat er mogelijk sprake is van *medeverantwoordelijkheid* of *individuele verantwoordelijkheid.*

De bewerker bepaalt ook niet wat de middelen zijn waarmee de persoonsgegevens verwerkt worden. Wel is het toegestaan dat de bewerker als expert de nadere invulling/details van de middelen bepaalt. Soms is het immers nodig dat een bewerker met meer technische kennis van de verwerkingsmiddelen wordt ingeschakeld. Het is belangrijk om hier bij het opstellen van een bewerkersovereenkomst voldoende aandacht aan te besteden. Op het moment dat een bewerker teveel zeggenschap heeft over de middelen die gebruikt worden bij de verwerking is niet langer sprake van een verantwoordelijke-bewerkerrelatie maar van *medeverantwoordelijkheid*.

**VOORBEELD**

EEN WONINGCORPORATIE WERKT SAMEN MET EEN AANNEMER/INSTALLATEUR OM ONDERHOUD/INSTALLATIEWERKZAAMHEDEN TE VERRICHTEN BIJ KLANTEN. DE WONINGCORPORATIE IS VERANTWOORDELIJKE VOOR DE PERSOONSGEGEVENS DIE ZIJ ONDER ZICH HEEFT. DE AANNEMER/INSTALLATEUR IS GEEN BEWERKER OMDAT HIJ NIET PRIMAIR WORDT INGESCHAKELD OM DE PERSOONSGEGEVENS TE GEBRUIKEN, MAAR OM ONDERHOUD/INSTALLATIEWERKZAAMHEDEN UIT TE VOEREN. HIERDOOR IS DE AANNEMER/INSTALLATEUR GEEN BEWERKER, MAAR MEDEVERANTWOORDELIJKE.

**Zonder aan zijn rechtstreeks gezag te zijn onderworpen**

De bewerker mag niet aan het rechtstreeks gezag van de verantwoordelijke onderworpen zijn. Een bewerker is dus altijd een *externe* partij en nooit een werknemer van de verantwoordelijke.

## VERANTWOORDELIJKHEDEN VAN DE BEWERKER

Onder de Wbp is de bewerker primair gebonden aan de vereisten die verantwoordelijke aan de verwerking stelt. Deze verplichtingen worden normaliter opgenomen in een bewerkersovereenkomst.
De bewerker heeft onder de AVG nieuwe verantwoordelijkheden gekregen die verder strekken dan zijn verantwoordelijkheden onder de Wbp en voor een groot deel overeenkomen met die van de verantwoordelijke. Deze verantwoordelijkheden zijn onder andere opgenomen in artikel 28 AVG.
De bewerker draagt er zorg voor dat:

- sprake is van passende technische en organisatorische maatregelen om de persoonsgegevens te beschermen (artikel 28 lid 1, 3 sub e en 4/artikel 32 AVG)
- geen gebruik wordt gemaakt van een andere (sub-)bewerker zonder schriftelijke toestemming van de verantwoordelijke (artikel 28 lid 2 en 4 AVG)
- goede procedures zijn ingericht om de verantwoordelijke te ondersteunen bij het behartigen van de rechten van betrokkenen
- na voltooiing van de werkzaamheden die in opdracht de van verantwoordelijke worden verricht de betreffende persoonsgegevens worden teruggegeven of vernietigd
- te allen tijde alle documentatie die nodig is om compliance met de wet aan te tonen aan de verantwoordelijke kan worden verstrekt
- hij de verantwoordelijke onmiddellijk informeert op het moment dat hij van mening is dat diens instructies in strijd zijn met de wet (artikel 28 lid 3 sub h AVG)
- in ieder geval al het personeel dat met persoonsgegevens moet werken onderworpen is aan een geheimhoudingsplicht (artikel 28 lid 3 sub b AVG/artikel 29 AVG)
- een overzicht wordt bijgehouden van alle categorieën van verwerkingsactiviteiten die voor de verantwoordelijke worden uitgevoerd (Documentatieplicht) (artikel 30 lid 2 AVG). Dit register bevat onder andere:
  - de naam en contactgegevens van de bewerkers en verantwoordelijken waarvoor de bewerker persoonsgegevens verwerkt
  - de categorieën van verwerkingen die voor elke verantwoordelijke worden uitgevoerd (denk hierbij bijvoorbeeld aan de categorieën opslag, analyse, doorgifte, et cetera)
  - eventuele documentatie met betrekking tot doorgifte van gegevens aan landen buiten de EU/EER
  - indien mogelijk een algemene beschrijving van de technische en organisatorische maatregelen die genomen zijn om de beveiliging van de persoonsgegevens te waarborgen.
- indien daar om wordt verzocht, medewerking wordt verleend aan de Autoriteit Persoonsgegevens (artikel 31 AVG)
- datalekken zonder vertraging worden gemeld aan de verantwoordelijke (artikel 33 lid 2 AVG)
- indien nodig een functionaris Gegevensbescherming wordt aangesteld (artikel 37 AVG)
- bij grensoverschrijdende gegevensoverdracht naar derde landen de regels van de AVG in acht worden genomen (artikel 44 AVG).

## DE BEWERKERSOVEREENKOMST (AVG: VERWERKERSOVEREENKOMST)

Een overeenkomst tussen een verantwoordelijke en een bewerker wordt bewerkersovereenkomst genoemd. In een dergelijke overeenkomst worden de rechten en plichten die de verantwoordelijke en de bewerker over en weer hebben op een rij gezet. Het sluiten van een bewerkersovereenkomst is zowel in de Wbp als in de AVG verplicht gesteld (artikel 14 lid 2 Wbp en artikel 28 lid 3 AVG), maar ook heel handig. Op het moment dat de verplichtingen goed zijn vastgelegd voorkomt dit namelijk dat hier op een later moment discussies over ontstaan.
Een bewerkersovereenkomst moet in ieder geval de volgende onderdelen bevatten:

- definiëring van begrippen.
- totstandkoming, duur en beëindiging van de overeenkomst
- vaststelling van het soort persoonsgegevens dat verwerkt wordt
- vaststelling van het soort verwerkingen
- beveiligingsmaatregelen
- export van persoonsgegevens buiten de EU/EER
- geheimhouding van persoonsgegevens
- procedure met betrekking tot datalekken
- aansprakelijkheidsclausules indien er inbreuk wordt gemaakt op de afspraken in de bewerkersovereenkomst

- bepaling omtrent teruggave van persoonsgegevens na afloop van de bewerkersovereenkomst en de bewaartermijn van persoonsgegevens.

Aan het eind van deze handreiking is een modelbewerkersovereenkomst opgenomen. Deze modelbewerkersovereenkomst bevat de bovenstaande onderdelen en kan nog nader worden aangevuld indien nodig.

# PRAKTIJKSITUATIES/Q&A

In dit onderdeel zal kort worden ingegaan op de onderstaande praktijksituaties. Er zal worden toegelicht met wat voor juridische constructie partijen te maken hebben, en wat zij hiervoor contractueel moeten regelen.

1. Traditionele relatie: Opdrachtgever (woningbouwcorporatie) geeft opdracht aan opdrachtnemer (aannemer/installateur et cetera) waarbij persoonsgegevens worden verstrekt.

   *Hier is sprake van medeverantwoordelijkheid, aangezien de opdrachtnemer niet zozeer wordt ingeschakeld om de persoonsgegevens te gebruiken, maar om werkzaamheden uit te voeren. Dit betekent dat voor het gebruik dat onder het beheer van de opdrachtnemer plaatsvindt de opdrachtnemer verantwoordelijke is. De opdrachtgever blijft verantwoordelijke voor het verstrekken van de persoonsgegevens aan de opdrachtnemer.*

   **Actie:**
   Zorg dat door zowel opdrachtgever als opdrachtnemer zorgvuldig wordt omgegaan met persoonsgegevens. Neem hiervoor de standaardbepalingen met betrekking tot privacy op in de algemene voorwaarden, overeenkomst of inkoopvoorwaarden.
   Als de behoefte bestaat om bepaalde zaken met betrekking tot de verwerking van persoonsgegevens gedetailleerder te regelen, sluit dan een overeenkomst met betrekking tot medeverantwoordelijkheid af.

2. Ontzorgende relatie: Opdrachtgever geeft opdracht aan opdrachtnemer waarbij opdrachtnemer gegevens in eigen beheer neemt vanwege de duur van de opdracht (bijvoorbeeld bij een meerjarig onderhoudscontract).

   *Hier is sprake van individuele verantwoordelijkheid. De opdrachtgever blijft verantwoordelijke voor de gegevens in zijn eigen beheer, maar de opdrachtnemer wordt afzonderlijke verantwoordelijke voor het gedeelte dat hij onder zich heeft gekregen. Hier hoeft dan ook geen extra overeenkomst voor worden afgesloten. Wel is het aan te raden om in de overeenkomst van opdracht een clausule op te nemen waaruit blijkt dat de betreffende gegevens na afloop van de overeenkomst worden teruggegeven. Dit om te voorkomen dat gegevens gaan rondzwerven.*

   **Actie:**
   Zorg dat er een clausule met betrekking tot teruggave van gegevens wordt opgenomen in de overeenkomst tot opdracht.

3. Ondergeschikte relatie: De opdrachtnemer sluit een nadere overeenkomst met een tweede opdrachtnemer, bijvoorbeeld een onderaannemer.

   *Deze situatie komt overeen met de traditionele situatie onder 1.*

4. Is er een bewerkersovereenkomst nodig indien een aannemer bij een klein aantal woningen (circa 20) onderhoudswerkzaamheden uitvoert en daarvoor de namen, adressen en telefoonnummers van de huurders ontvangt?

   *Hier is sprake van een situatie van medeverantwoordelijkheid zoals hierboven beschreven. De hoeveelheid persoonsgegevens is niet leidend als het gaat om de verhouding die partijen met elkaar hebben.*

   **Actie:**
   Neem de standaardbepalingen met betrekking tot privacy op in de algemene voorwaarden, overeenkomst of inkoopvoorwaarden of sluit een overeenkomst met betrekking tot medeverantwoordelijkheid af.

5. Situatie waarin sprake is van het verstrekken van gegevens van werknemers aan een opdrachtgever, zodat werknemers kunnen worden toegelaten op het terrein van de opdrachtgever.

*In deze situatie is er sprake van een verantwoordelijke-bewerkerrelatie. De opdrachtnemer levert in de hoedanigheid van bewerker de gegevens van haar medewerkers. De klant zelf (de opdrachtgever) is verantwoordelijke met betrekking tot het verwerken van de persoonsgegevens voor het verschaffen van toegang. De opdrachtgever is in dit geval dus ook verantwoordelijk voor het hebben van een goede grondslag voor het verwerken van persoonsgegevens. Door de afhankelijkheidsrelatie is 'toestemming' hier niet voldoende.*

**Actie:**
Sluit een bewerkersovereenkomst af met de opdrachtgever in aanvulling op de hoofdovereenkomst, waarin duidelijk wordt afgebakend wat wel en niet toegestaan is met de persoonsgegevens van de werknemers. Geef in de onderhandelingen aan dat een goede grondslag voor het verwerken van persoonsgegevens een wettelijke verplichting is en dat de verantwoordelijke hieraan dient te voldoen.

# BIJLAGEN

## 1 MODEL BEWERKERSOVEREENKOMST

**Bewerkersovereenkomst** [NAAM BEDRIJF]
**Datum:** [INVOEREN DATUM]

**Contractpartijen:**
1. Verantwoordelijke te weten [STATUTAIRE NAAM], statutair gevestigd te [PLAATS], vertegenwoordigd door [NAAM EN/OF NAAM BESTUURDER]

hierna te noemen: **'Verantwoordelijke',**

en

2. Verwerker te weten [STATUTAIRE NAAM], statutair gevestigd te [PLAATS], vertegenwoordigd door [NAAM EN/OF NAAM BESTUURDER]

hierna te noemen: **'Bewerker',**

gezamenlijk aan te duiden als: **'Partijen';**

**Overwegende dat:**

Partijen hebben op [DATUM] een Overeenkomst met betrekking tot [OMSCHRIJVING] gesloten. Ter uitvoering van deze Overeenkomst worden Persoonsgegevens verwerkt.
Verantwoordelijke hecht grote waarde aan het beschermen van deze Persoonsgegevens. Om die reden leggen Partijen in deze Bewerkersovereenkomst en de daarbij behorende bijlagen, te weten:
1. overzicht met verwerkingen van Persoonsgegevens en verwerkingsdoelen
2. overzicht met beveiligingsmaatregelen
3. proces rondom het melden van Datalekken en de te verstrekken informatie met betrekking tot het Datalek vast wat Bewerker wel en niet mag doen met de Persoonsgegevens.

### 1. DEFINITIES

De hierna en hiervoor gebruikte begrippen volgen uit de Algemene Verordening Gegevensbescherming en hebben de volgende betekenis:

1.1 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (**'de Betrokkene'**); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of mee elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

1.2 Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

1.3 Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van Persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen (**'Verantwoordelijke'**).

1.4 Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke Persoonsgegevens verwerkt (**'Bewerker'**).
1.5 Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte Persoonsgegeven betrekking hebben.
1.6 Verwerkersovereenkomst: deze Overeenkomst inclusief de bijlagen (**'Bewerkersovereenkomst'**).
1.7 Overeenkomst: de hoofdovereenkomst waar deze Bewerkersovereenkomst uit voortvloeit.
1.8 Inbreuk in verband met Persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens (**'Datalek'**).
1.9 Toezichthoudende autoriteit: een onafhankelijke overheidsinstantie verantwoordelijk voor het toezicht op de naleving van de wet in verband met de verwerking van Persoonsgegevens. In Nederland is dit de Autoriteit Persoonsgegevens.

## 2. TOTSTANDKOMING, DUUR EN BEËINDIGING VAN DEZE BEWERKERSOVEREENKOMST

2.1 Deze Bewerkersovereenkomst treedt in werking op de datum waarop Partijen deze ondertekenen.
2.2 Deze Bewerkersovereenkomst is onderdeel van de Overeenkomst en zal gelden voor zolang de Overeenkomst duurt.
2.3 Indien de Overeenkomst eindigt, eindigt deze Bewerkersovereenkomst automatisch; de Bewerkersovereenkomst kan niet apart worden opgezegd.
2.4 Na beëindiging van deze Bewerkersovereenkomst zullen de lopende verplichtingen voor Bewerker, zoals het melden van Datalekken waarbij Persoonsgegevens van Verantwoordelijke betrokken zijn en de plicht tot geheimhouding blijven voortduren.

## 3. VERWERKEN PERSOONSGEGEVENS

3.1 Bewerker verwerkt alleen Persoonsgegevens in opdracht van Verantwoordelijke en Bewerker heeft geen zeggenschap over de Persoonsgegevens. Bewerker volgt instructies van Verantwoordelijke ten aanzien van de verwerking op en mag de Persoonsgegevens niet op een andere manier verwerken, tenzij Verantwoordelijke Bewerker daar van tevoren toestemming of opdracht voor geeft.
3.2 In Bijlage 1 wordt opgenomen welke Persoonsgegevens Bewerker precies zal verwerken en voor welke verwerkingsdoeleinden.
3.3 Bewerker houdt zich aan de wet en verwerkt de gegevens op een behoorlijke, zorgvuldige en transparante wijze.
3.4 Bewerker mag zonder voorafgaande schiftelijke toestemming van Verantwoordelijke geen andere personen of organisaties inschakelen bij het verwerken van de Persoonsgegevens.
3.5 Wanneer Bewerker met toestemming van Verantwoordelijke andere organisaties inschakelt, moeten zij minimaal voldoen aan de eisen die zijn opgenomen in deze Bewerkersovereenkomst.
3.6 Wanneer Verantwoordelijke een verzoek van een Betrokkene ontvangt ten aanzien van het uitoefenen van zijn of haar rechten, dan werkt Bewerker daar binnen een termijn van 14 dagen aan mee. Deze rechten bestaan uit een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming, bezwaar maken tegen de verwerking van de Persoonsgegevens en een verzoek tot overdraagbaarheid van de eigen Persoonsgegevens.

## 4. BEVEILIGEN PERSOONSGEGEVENS

4.1 Bewerker zorgt ervoor dat de Persoonsgegevens voldoende worden beveiligd. Om verlies en onrechtmatige verwerkingen te voorkomen neemt Bewerker passende technische en organisatorische maatregelen.
4.2 Deze maatregelen zijn afgestemd op het risico van de Verwerking. Een overzicht van deze maatregelen en het beleid daaromtrent wordt opgenomen in Bijlage 2.
4.3 Ter controle van de genomen beveiligingsmaatregelen zal Bewerker aan Verantwoordelijke ieder jaar een rapportage sturen waarin de genomen maatregelen staan en de eventuele aandachts- en/of verbeterpunten. Hiervoor brengt Bewerker geen kosten in rekening aan Verantwoordelijke.

4.4 Verantwoordelijke mag een audit laten uitvoeren om te bepalen of het verwerken van de Persoonsgegevens aan de wet en de afspraken uit deze Bewerkersovereenkomst voldoet. Bewerker verleent hierbij zijn medewerking. Waaronder het toegang verlenen tot gebouwen en databases en het ter beschikking stellen van alle relevante informatie.
4.5 De kosten voor de uitvoering van deze audit zullen voor rekening van Bewerker komen wanneer blijkt dat Bewerker zich niet aan de verplichtingen in deze Bewerkersovereenkomst houdt.
4.6 De controle op de algehele verwerking van Persoonsgegevens door Bewerker kan, naast de auditmogelijkheid, ook geschieden via zelfevaluatie door Bewerker. Bewerker zal hierbij aan Verantwoordelijke een rapport verstrekken waarin Bewerker aantoont dat hij voldoet aan de wet en de afspraken uit deze Bewerkersovereenkomst. Deze rapportage dient te worden ondertekend door een directielid binnen de organisatie van Bewerker.
4.7 Wanneer Partijen vinden dat een wijziging in de te nemen beveiligingsmaatregelen noodzakelijk is, treden Partijen in overleg over de wijziging daarvan. De kosten gemoeit met het wijzigen van de beveiligingsmaatregelen komen voor rekening van degene die de kosten maakt.

## 5. EXPORTEREN PERSOONSGEGEVENS

5.1 Bewerker mag geen Persoonsgegevens laten verwerken door andere personen of organisaties buiten de Europese Economische Ruimte (EER), zonder daarvoor voorafgaande schriftelijke toestemming te hebben verkregen van Verantwoordelijke.

## 6. GEHEIMHOUDING

6.1 Bewerker zal de verstrekte Persoonsgegevens geheim houden, tenzij dit op basis van een wettelijke verplichting niet kan.
6.2 Bewerker zorgt dat zijn/haar personeel en ingeschakelde hulppersonen zich aan deze geheimhouding houden, door een geheimhoudingsplicht in de (arbeids-)contracten op te nemen.

## 7. DATALEKKEN

7.1 In geval van een ontdekking van een mogelijk Datalek zal Bewerker Verantwoordelijke hierover informeren binnen een termijn van 24 uur overeenkomstig het proces volgend uit Bijlage 3, zodat Verantwoordelijke indien nodig een melding van het Datalek bij de Toezichthouder kan doen. De Bewerker zal niet op eigen initiatief melding van het Datalek doen bij de Toezichthouder.
7.2 Bewerker zal Verantwoordelijke op de hoogte houden van nieuwe ontwikkelingen rondom het Datalek, ook zal Bewerker de getroffen maatregelen om het Datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen, overleggen aan Verantwoordelijke.
7.3 Bewerker mag geen melding van een Datalek aan de Toezichthouder doen, wanneer bij het Datalek Persoonsgegevens van Verantwoordelijke betrokken zijn. Ook mag Bewerker de Betrokkenen niet informeren over het Datalek. Deze verantwoordelijkheid ligt bij Verantwoordelijke.
7.4 Eventuele kosten die gemaakt worden om het Datalek op te lossen en in de toekomst te kunnen voorkomen, komen voor rekening van degene die de kosten maakt.

## 8. AANSPRAKELIJKHEID

8.1 Als Bewerker de verplichtingen uit deze Bewerkersovereenkomst niet nakomt, kan Verantwoordelijke Bewerker daarvoor aansprakelijk stellen.
8.2 Bewerker is aansprakelijk voor alle schade die Verantwoordelijke lijdt door het niet nakomen van de wet en de bepalingen uit deze Bewerkersovereenkomst, voor zover dit is ontstaan door de werkzaamheden van Bewerker.
8.3 Indien Bewerker de verplichtingen in deze Bewerkersovereenkomst overtreedt, is Bewerker aan *Verantwoordelijke een direct opeisbare boete verschuldigd van [BEDRAG] voor iedere overtreding en [BEDRAG] voor iedere dag dat Bewerker de overtreding begaat. Daarnaast behoudt Verantwoordelijke het recht om schadevergoeding te vorderen.* (optioneel)

8.4 Bewerker is aansprakelijk voor de aan Verantwoordelijke opgelegde bestuurlijke boete door de Toezichthouder als de schade het gevolg is van het onrechtmatig of nalatig handelen van Bewerker.
8.5 Verantwoordelijke is niet aansprakelijk voor aanspraken van Betrokkene of andere personen en organisaties waar Bewerker de samenwerking mee is aangegaan of waarvan Bewerker Persoonsgegevens verwerkt, als dit het gevolg is van het onrechtmatig of nalatig handelen van Bewerker.

## 9. TERUGGAVE PERSOONSGEGEVENS EN BEWAARTERMIJN

9.1 Na het beëindigen van deze Bewerkersovereenkomst geeft Bewerker de Persoonsgegevens terug aan Verantwoordelijke.
9.2 De overgebleven Persoonsgegevens zal Bewerker vernietigen na verstrijken van de wettelijke bewaartermijn en/of op verzoek van Verantwoordelijke. Hierbij valt bijvoorbeeld te denken aan Persoonsgegevens die om belastingtechnische redenen bewaard moeten blijven.

## 10. SLOTBEPALINGEN

10.1 Deze Bewerkersovereenkomst is onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst zijn daarom ook van toepassing op de Bewerkersovereenkomst.
10.2 Bij eventuele tegenstrijdigheden tussen de bepalingen in de Bewerkersovereenkomst en de Overeenkomst, gelden de bepalingen uit deze Bewerkersovereenkomst ten aanzien van de verwerking van Persoonsgegevens.
10.3 Afwijkingen van deze Bewerkersovereenkomst zijn slechts geldig wanneer Partijen dit samen schriftelijk afspreken.

**Aldus door Partijen overeengekomen en ondertekend:**

**Verantwoordelijke:**
Ondertekend voor en namens [STATUTAIRE NAAM]
Naam:
Functie:
Datum en plaats:
Handtekening:

**Bewerker:**
Ondertekend voor en namens [STATUTAIRE NAAM]
Naam:
Functie:
Datum en plaats:
Handtekening:

## BIJLAGE 1 OVERZICHT MET VERWERKINGEN VAN PERSOONSGEGEVENS EN VERWERKINGSDOELEN

Het onderstaande schema zal ingevuld moeten worden elke keer dat een Bewerkersovereenkomst wordt gesloten. Het geeft een volledig overzicht van de Persoonsgegevens die verwerkt zullen worden. Dit maakt het makkelijker om aan te kunnen tonen waar, door wie en voor welk doel de Persoonsgegevens worden verwerkt.

| | |
|---|---|
| Beschrijving verwerkingsactiviteiten door bewerker: | |
| Verwerkingsdoelen: | |
| Verantwoordelijke: | |
| Bewerker: | |
| Subbewerkers: | |
| Verwerkte Persoonsgegevens: | |
| Locatie verwerkingen: | |
| Bewaartermijn: | |

## BIJLAGE 2 OVERZICHT MET BEVEILIGINGSMAATREGELEN

Overzicht van de beveiligingsnormen die de Verantwoordelijke aan de Bewerker oplegt.
Om vast te stellen wat passende beveiligingsmaatregelen zijn, moet een afweging worden gemaakt op basis van de risico's van de verwerking aan de hand van onder meer de volgende punten:

- Het soort Persoonsgegevens dat verwerkt wordt (normaal, bijzonder of gevoelig) en eventueel de daarbij behorende (risico)classificatie die de organisatie zelf aan de gegevens heeft gegeven. *Gaat het bijvoorbeeld om een naam of een e-mailadres, wat minder gevoelige Persoonsgegevens zijn, of gaat het om het verwerken van een BSN.*
- De hoeveelheid betrokkenen van wie gegevens worden verwerkt. *Hoe meer betrokkenen er zijn, hoe meer eisen er worden gesteld aan de beveiliging van de gegevens.*
- Het doel waarvoor gegevens worden verwerkt.
- De duur en de wijze waarop gegevens bewaard moeten worden.

Er kan vervolgens onderscheid gemaakt worden tussen organisatorische beveiligingseisen, zoals het voorkomen van diefstal van een laptop met daarop Persoonsgegevens uit de auto, en technische beveiligingseisen, zoals een uitgebreide IT-omgeving die beveiligd wordt tegen virussen en waar encryptie van de gegevens wordt toegepast. Van een grote organisatie wordt meer verwacht ten aanzien van de te nemen beveiligingseisen.

De onderstaande maatregelen zijn suggesties voor beveiligingsmaatregelen en de aanwezigheid hiervan kan een indicatie zijn van een gepast beveiligingsniveau.

**Technische beveiligingsmaatregelen**

☐ Up-to-date virusscanner op elke laptop, pc en tablet
☐ Beveiligde USB-sticks
☐ Accurate beveiliging medewerkerstelefoon
☐ Bitlocker toegangsmechanisme
☐ Unieke inlogcode en wachtwoord (regelmatig aanpassen)
☐ Versleutelde e-mail
☐ Geen onbeveiligde externe harde schijven
☐ Geen onbeveiligde back-ups maken
☐ Geen documenten op privélaptop opslaan

**Organisatorische beveiligingsmaatregelen**

☐ Clean desk policy
☐ Laptop niet onbemand achterlaten
☐ Laptop nooit achterlaten in de auto
☐ Privacy screens medewerkers
☐ Oude documenten op juiste manier vernietigen
☐ Zorgvuldig gebruik van USB-sticks

## BIJLAGE 3 PROCES RONDOM HET MELDEN VAN DATALEKKEN EN DE TE VERSTREKKEN INFORMATIE

**Wat is een beveiligingsincident en wanneer moet dit gemeld worden?**
Een datalek is een beveiligingsincident waarbij Persoonsgegevens, die de Bewerker namens de Verantwoordelijke beheert, mogelijk verloren zijn gegaan of onbedoeld toegankelijk waren voor derden. Het gaat om gegevens die te koppelen zijn aan deze personen, zoals, maar niet beperkt tot, namen, adressen, telefoonnummers, e-mailadressen, login-gegevens, cookies, IP-adressen of identificerende gegevens van computers of telefoons.

Hieronder vind je een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de Autoriteit Persoonsgegevens.
- De website met login-gegevens is gehackt of is toegankelijk voor derden.
- Verlies van een laptop of USB-stick met Persoonsgegevens.
- Salarisstroken van medewerkers zijn per ongeluk naar verkeerde personen gestuurd.
- Brieven of e-mails worden naar een verkeerd adres gestuurd.
- Een aanval van een hacker op het ICT-systeem.
- Een verloren of gestolen telefoon waar Persoonsgegevens op aanwezig zijn.

**Wat te doen bij twijfel?**
Als je op basis van bovenstaande niet zeker weet of er sprake is van een beveiligingsincident, stel je jezelf in ieder geval alvast de volgende vragen als hulpmiddel:
- Is er een technisch of fysiek beveiligingsprobleem?
- Gaat het probleem over de beveiliging van Persoonsgegevens? Ook IP-adressen, telefoonnummers of identificerende gegevens, bijvoorbeeld van hardware, kunnen hieronder vallen.
- Gaat het om gevoelige gegevens zoals ras, gezondheidsgegevens, informatie over iemands financiële situatie, zoals salaris of gegevens waar (identiteit)fraude mee kan worden gepleegd, zoals een Burgerservicenummer?
- Zijn er grote hoeveelheden Persoonsgegevens onbedoeld toegankelijk geworden voor derden?
- Gaat het om gegevens van kwetsbare groepen zoals kinderen?
- Worden de Persoonsgegevens beheerd door een leverancier?
- Ook wanneer je twijfelt, neem het zekere voor het onzekere en neem altijd contact op met de [invoeren naam contactpersoon of afdeling].

**Waar meld je het beveiligingsincident?**
Als je een beveiligingsincident hebt ontdekt, neem je direct contact op met de [invoeren naam contactpersoon of afdeling]:

Telefoon: [invoeren telefoonnummer]
Of
E-mail: [invoeren e-mailadres]

**Geef in je e-mail beantwoording op de onderstaande vragen**
Wij willen graag dat je de onderstaande vragen voor ons beantwoord. Deze vragen zijn gelijk aan de informatie die aan de Autoriteit Persoonsgegevens moet worden verstrekt.

De [invoeren naam contactpersoon of afdeling] kan je helpen met de beantwoording hiervan. Gaarne de vragen zo volledig mogelijk en schriftelijk beantwoorden.

1. Geef een samenvatting van het beveiligingslek/beveiligingsincident/datalek: wat is er gebeurd?
   Vermeld hier ook de naam van het betrokken systeem.
2. Welke typen Persoonsgegevens zijn betrokken bij het beveiligingsincident?
   Zoals, maar niet beperkt tot, naam, adres, e-mailadres, IP-nummer, Burgerservicenummer, pasfoto en ieder ander tot een persoon te herleiden gegeven.
3. Van hoeveel personen zijn de Persoonsgegevens betrokken bij het beveiligingsincident?
   Geef a.u.b. een minimum en maximum aantal personen.

4. Omschrijving groep personen om wiens gegevens het gaat.
   Geef aan of het gaat om medewerkersgegevens, gegevens van internetgebruikers. Bijzondere aandacht verdienen gegevens van een kwetsbare groepen personen, zoals kinderen.
5. Zijn de contactgegevens van de betrokken personen bekend?
   Het kan zijn dat betrokkenen geïnformeerd moeten worden over het datalek, kunnen we deze personen in dat geval bereiken?
6. Wat is de oorzaak (root cause) van het beveiligingsincident?
   Heeft u een idee hoe het beveiligingsincident heeft kunnen ontstaan?
7. Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden?
   Geef dit a.u.b. zo specifiek mogelijk aan.

## 2 MODELREGELING GEZAMENLIJKE VERANTWOORDELIJKHEID

**Modelregeling Gezamenlijke verantwoordelijkheid** [NAAM BEDRIJVEN]

**Datum:** [INVOEREN DATUM]

**CONTRACTPARTIJEN:**

1. Medeverantwoordelijke te weten [STATUTAIRE NAAM], statutair gevestigd te [PLAATS], vertegenwoordigd door [NAAM EN/OF NAAM BESTUURDER]

hierna te noemen: **'Medeverantwoordelijke 1'**,

en

2. Medeverantwoordelijke te weten [STATUTAIRE NAAM], statutair gevestigd te [PLAATS], vertegenwoordigd door [NAAM EN/OF NAAM BESTUURDER]

hierna te noemen: **'Medeverantwoordelijke 2'**,

gezamenlijk aan te duiden als: **'Partijen'**;

**Overwegende dat:**

Partijen hebben op [DATUM] een Overeenkomst met betrekking tot [OMSCHRIJVING] gesloten. Ter uitvoering van deze Overeenkomst worden Persoonsgegevens verwerkt.
Partijen hechten grote waarde aan het beschermen van deze Persoonsgegevens. Om die reden leggen Partijen in deze Modelregeling Gezamenlijke verantwoordelijkheid en de daarbij behorende bijlagen, te weten:
1. overzicht met verwerkingen van Persoonsgegevens en verwerkingsdoelen
2. proces rondom het melden van Datalekken en de te verstrekken informatie en de wederzijdse verantwoordelijkheden vast.

### 1. DEFINITIES

De hierna en hiervoor gebruikte begrippen volgen uit de Algemene Verordening Gegevensbescherming en hebben de volgende betekenis:

1.1 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de Betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

1.2 Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

1.3 Gezamenlijke verantwoordelijkheid: wanneer twee of meer verantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijkverantwoordelijk.

1.4 Verantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van Persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verantwoordelijke is of volgens welke criteria deze wordt aangewezen.

1.5 Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte Persoonsgegevens betrekking hebben.
1.6 Overeenkomst: de hoofdovereenkomst waar deze Modelregeling Gezamenlijke verantwoordelijkheid uit voortvloeit.
1.7 Inbreuk in verband met Persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens (**'Datalek'**).
1.8 Toezichthoudende autoriteit: een onafhankelijke overheidsinstantie verantwoordelijk voor het toezicht op de naleving van de wet in verband met de verwerking van Persoonsgegevens. In Nederland is dit de Autoriteit Persoonsgegevens.

## 2. TOTSTANDKOMING, DUUR EN BEËINDIGING VAN DEZE MODELREGELING GEZAMENLIJKE VERANTWOORDELIJKHEID

2.1 Deze Modelregeling Gezamenlijke verantwoordelijkheid treedt in werking op de datum waarop Partijen deze ondertekenen.
2.2 Deze Modelregeling Gezamenlijke verantwoordelijkheid is onderdeel van de Overeenkomst en zal gelden voor zolang de Overeenkomst duurt.
2.3 Indien de Overeenkomst eindigt, eindigt deze Modelregeling Gezamenlijke verantwoordelijkheid automatisch; de Modelregeling Gezamenlijke verwerkingsverantwoordelijken kan niet apart worden opgezegd.
2.4 Na beëindiging van deze Modelregeling Gezamenlijke verantwoordelijkheid zullen de lopende verplichtingen, zoals het melden van Datalekken waarbij Persoonsgegevens van Partijen zijn betrokken en de plicht tot geheimhouding blijven voortduren.

## 3. VERWERKEN PERSOONSGEGEVENS

3.1 Partijen verwerken Persoonsgegevens alleen op de wijze zoals Partijen dit bij deze Modelregeling Gezamenlijke verantwoordelijkheid overeenkomen en zullen Persoonsgegevens niet op een andere manier verwerken, tenzij Partijen dit gezamenlijk overeenkomen.
3.2 In Bijlage 1 wordt opgenomen welke Persoonsgegevens Partijen precies zullen verwerken, voor welke verwerkingsdoeleinden en wie voor welk deel verantwoordelijk is.
3.3 Partijen houden zich bij het verwerken van Persoonsgegevens aan de wet en de gegevens worden verwerkt op een behoorlijke, zorgvuldige en transparante wijze.
3.4 Partijen mogen zonder voorafgaande schriftelijke toestemming van elkaar geen andere personen of organisaties inschakelen bij het verwerken van de Persoonsgegevens.
3.5 Wanneer Partijen met toestemming van elkaar andere organisaties inschakelen, moeten zij minimaal voldoen aan de eisen die zijn opgenomen in deze Modelregeling Gezamenlijke verantwoordelijkheid.
3.6 Wanneer Partijen een verzoek van een Betrokkene ontvangen ten aanzien van het uitoefenen van zijn of haar rechten, zullen Partijen voor het deel waar zij verantwoordelijk voor zijn, zorgen dat de Betrokkene zijn of haar rechten effectief kan uitoefenen. Deze rechten bestaan uit een verzoek om inzage, correctie, aanvulling, verwijdering of afscherming, bezwaar maken tegen de verwerking van de Persoonsgegevens en een verzoek tot overdraagbaarheid van de eigen Persoonsgegevens.
3.7 Partijen dienen op duidelijke en eenvoudige wijze te communiceren waar de Betrokkene voor het uitoefenen van zijn rechten terecht kan. Hierbij geven partijen aan welke Medeverantwoordelijken er zijn en wie voor welk deel verantwoordelijk is.

## 4. EXPORTEREN PERSOONSGEGEVENS

4.1 Partijen mogen geen Persoonsgegevens laten verwerken door andere personen of organisaties buiten de Europese Economische Ruimte (EER), zonder daarvoor voorafgaande schriftelijke toestemming te hebben verkregen van de andere Medeverantwoordelijke.

## 5. GEHEIMHOUDING

5.1 Partijen zullen de verstrekte Persoonsgegevens geheim houden, tenzij dit op basis van een wettelijke verplichting niet kan.
5.2 Partijen zorgen ervoor dat het personeel en ingeschakelde hulppersonen zich aan deze geheimhouding houden, door een geheimhoudingsplicht in de (arbeids-)contracten op te nemen.

## 6. DATALEKKEN

6.1 In geval van een ontdekking van een mogelijk Datalek zullen Partijen elkaar hierover informeren binnen 24 uur overeenkomstig de procedure zoals die is opgenomen in Bijlage 2.
6.2 Partijen zullen elkaar op de hoogte houden van nieuwe ontwikkelingen rondom het Datalek, ook zullen Partijen de getroffen maatregelen om het Datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen, overleggen aan elkaar.
6.3 Partijen doen elk voor dat deel waar zij verantwoordelijk voor zijn de melding van een Datalek bij de Toezichthouder. Hetzelfde geldt voor de melding aan de Betrokkenen.
6.4 Eventuele kosten die gemaakt worden om het Datalek op te lossen en in de toekomst te kunnen voorkomen, komen voor rekening van degene die de kosten maakt.

## 7. AANSPRAKELIJKHEID

7.1 Als een van de Partijen de verplichtingen uit deze Modelregeling Gezamenlijke verantwoordelijkheid niet nakomt, kunnen zij voor hun deel van de verwerking aansprakelijk gesteld worden.
7.2 *Indien een van de Partijen de verplichtingen ten aanzien van zijn/haar deel in deze Modelregeling Gezamenlijke verantwoordelijkheid niet nakomt, is de ene Medeverantwoordelijke aan de andere Medeverantwoordelijke een direct opeisbare boete verschuldigd van [BEDRAG] voor iedere niet-nakoming en [BEDRAG] voor iedere dag dat de Medeverantwoordelijke de verplichtingen niet nakomt. Daarnaast behouden Partijen het recht om aanvullende schadevergoeding te vorderen.* (optioneel)
7.3 De ene Medeverantwoordelijke is aansprakelijk voor de aan de andere Medeverantwoordelijke opgelegde bestuurlijke boete door de Toezichthoudende autoriteit als de schade het gevolg is van het onrechtmatig of nalatig handelen van die Medeverantwoordelijke.
7.4 De ene Medeverantwoordelijke is niet aansprakelijk voor aanspraken van Betrokkenen of andere personen en organisaties waar de andere Medeverantwoordelijke de samenwerking mee is aangegaan, als dit het gevolg is van het onrechtmatig of nalatig handelen van die Medeverantwoordelijke.

## 8. TERUGGAVE PERSOONSGEGEVENS EN BEWAARTERMIJN

8.1 Na het beëindigen van deze Modelregeling Gezamenlijke verantwoordelijkheid geven Partijen de Persoonsgegevens terug aan elkaar.
8.2 De overgebleven Persoonsgegevens zullen Partijen vernietigen na verstrijken van de wettelijke bewaartermijn.

## 9. SLOTBEPALINGEN

9.1 Deze Modelregeling Gezamenlijke verantwoordelijkheid is onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst zijn daarom ook van toepassing op deze Modelregeling Gezamenlijke verantwoordelijkheid.
9.2 Bij eventuele tegenstrijdigheden tussen de bepalingen in de Modelregeling Gezamenlijke verwerkingsverantwoordelijken en de Overeenkomst, gelden de bepalingen uit deze Modelregeling Gezamenlijke verantwoordelijkheid ten aanzien van de verwerking van Persoonsgegevens.
9.3 Afwijkingen van deze Modelregeling Gezamenlijke verantwoordelijkheid zijn slechts geldig wanneer Partijen dit samen schriftelijk overeenkomen.

**Aldus door Partijen overeengekomen en ondertekend:**

**Medeverantwoordelijke 1:**
Ondertekend voor en namens [STATUTAIRE NAAM]
Naam:
Functie:
Datum en plaats:
Handtekening:

**Medeverantwoordelijke 2:**
Ondertekend voor en namens [STATUTAIRE NAAM]
Naam:
Functie:
Datum en plaats:
Handtekening:

## BIJLAGE 1 OVERZICHT MET VERWERKINGEN VAN PERSOONSGEGEVENS EN VERWERKINGSDOELEN

Het onderstaande schema zal ingevuld moeten worden elke keer dat een Modelregeling Gezamenlijke verantwoordelijkheid wordt gesloten. Het geeft een volledig overzicht van de Persoonsgegevens die verwerkt zullen worden en voor welk deel van de Persoonsgegevens welke Medeverantwoordelijke verantwoordelijk is. Op basis van dit overzicht is het mogelijk om aan te kunnen tonen waar, door wie en voor welk doel de Persoonsgegevens worden verwerkt. Daarnaast is het ook mogelijk om op basis van dit overzicht de Betrokkenen te kunnen informeren dat hun Persoonsgegevens worden verwerkt zoals is vereist op grond van artikel 13 van de Algemene Verordening Gegevensbescherming.

| | |
|---|---|
| Beschrijving verwerkingsactiviteiten door Medeverantwoordelijke 1: | |
| Verwerkingsdoelen: | |
| Medeverantwoordelijke 1:<br>(naam, contactgegevens, contactgegevens van de functionaris Gegevensbescherming wanneer de organisatie een dergelijke functionaris heeft) | |
| Verwerkte Persoonsgegevens: | |
| Locatieverwerkingen: | |
| Subbewerkers: | |
| Bewaartermijn: | |

| | |
|---|---|
| Beschrijving verwerkingsactiviteiten door Medeverantwoordelijke 2: | |
| Verwerkingsdoelen: | |
| Medeverantwoordelijke 2:<br>(naam, contactgegevens, contactgegevens van de functionaris Gegevensbescherming wanneer de organisatie een dergelijke functionaris heeft) | |
| Verwerkte Persoonsgegevens: | |
| Locatieverwerkingen: | |
| Subbewerkers: | |
| Bewaartermijn: | |

## BIJLAGE 2 PROCES RONDOM HET MELDEN VAN DATALEKKEN EN DE TE VERSTREKKEN INFORMATIE

**Wat is een beveiligingsincident en wanneer moet dit gemeld worden?**
*Een Datalek is een beveiligingsincident waarbij Persoonsgegevens, die de ene Medeverantwoordelijke namens de andere Medeverantwoordelijke beheert, mogelijk verloren zijn gegaan of onbedoeld toegankelijk waren voor derden. Elke Medeverantwoordelijke dient voor het deel waar hij/zij verantwoordelijk voor is een melding te maken bij de Toezichthoudende autoriteit wanneer er sprake is van een beveiligingsincident. Het gaat om gegevens die te koppelen zijn aan personen, zoals, maar niet beperkt tot, namen, adressen, telefoonnummers, e-mailadressen, login-gegevens, cookies, IP-adressen of identificerende gegevens van computers of telefoons.*

Hieronder vind je een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de Autoriteit Persoonsgegevens:

- De website met login-gegevens is gehackt of is toegankelijk voor derden.
- Verlies van een laptop of USB-stick met persoonsgegevens.
- Salarisstroken van medewerkers zijn per ongeluk naar verkeerde personen gestuurd.
- Brieven of e-mails worden naar een verkeerd adres gestuurd.
- Een aanval van een hacker op het ICT-systeem.
- Een verloren of gestolen telefoon waar persoonsgegevens op aanwezig zijn.

**Wat te doen bij twijfel?**
Als je op basis van bovenstaande niet zeker weet of er sprake is van een beveiligingsincident, stel je jezelf in ieder geval alvast de volgende vragen als hulpmiddel:

- Is er een technisch of fysiek beveiligingsprobleem?
- Gaat het probleem over de beveiliging van Persoonsgegevens? Ook IP-adressen, telefoonnummers of identificerende gegevens, bijvoorbeeld van hardware zoals een IMEI-nummer, kunnen hieronder vallen.
- Gaat het om gevoelige gegevens zoals ras, gezondheidsgegevens, informatie over iemands financiële situatie, zoals salaris of gegevens waar (identiteits)fraude mee kan worden gepleegd, zoals een Burgerservicenummer?
- Zijn er grote hoeveelheden Persoonsgegevens onbedoeld toegankelijk geworden voor derden?
- Gaat het om gegevens van kwetsbare groepen zoals kinderen?
- Worden de Persoonsgegevens beheerd door een leverancier?

Ook wanneer je twijfelt, neem het zekere voor het onzekere en neem altijd contact op met:

Medeverantwoordelijke 1:
[invoeren naam contactpersoon of afdeling]

Medeverantwoordelijke 2:
[invoeren naam contactpersoon of afdeling]

**Waar meld je het beveiligingsincident?**
Als je een beveiligingsincident hebt ontdekt, neem je direct contact op met:

Medeverantwoordelijke 1:
[invoeren naam contactpersoon of afdeling]
Telefoon: [invoeren telefoonnummer]
Of
E-mail: [invoeren e-mailadres]

Medeverantwoordelijke 2:
[invoeren naam contactpersoon of afdeling]
Telefoon: [invoeren telefoonnummer]
Of
E-mail: [invoeren e-mailadres]

**Geef in je e-mail beantwoording op de onderstaande vragen**
De onderstaande vragen zijn gelijk aan de informatie die aan de Autoriteit Persoonsgegevens moet worden verstrekt wanneer er van het Datalek een melding gemaakt moet worden.

De [invoeren naam contactpersoon of afdeling] kan je helpen met de beantwoording hiervan. Gaarne de vragen zo volledig mogelijk en schriftelijk beantwoorden.

1. Geef een samenvatting van het beveiligingslek/beveiligingsincident/Datalek: wat is er gebeurd?
   Vermeld hier ook de naam van het betrokken systeem.
2. Welke typen Persoonsgegevens zijn betrokken bij het beveiligingsincident?
   Zoals, maar niet beperkt tot, naam, adres, e-mailadres, IP-nummer, Burgerservicenummer, pasfoto en ieder ander tot een persoon te herleiden gegeven.
3. Van hoeveel personen zijn de Persoonsgegevens betrokken bij het beveiligingsincident?
   Geef a.u.b. een minimum en maximum aantal personen.
4. Omschrijving groep personen om wiens gegevens het gaat.
   Geef aan of het gaat om medewerkersgegevens, gegevens van internetgebruikers. Bijzondere aandacht verdienen gegevens van kwetsbare groepen personen, zoals kinderen.
5. Zijn de contactgegevens van de betrokken personen bekend?
   Het kan zijn dat Betrokkenen geïnformeerd moeten worden over het Datalek, kunnen we deze personen in dat geval bereiken?
6. Wat is de oorzaak (root cause) van het beveiligingsincident?
   Heeft u een idee hoe het beveiligingsincident heeft kunnen ontstaan?
7. Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden?
   Geef dit a.u.b. zo specifiek mogelijk aan.

## 3 MODELBEPALING PRIVACY TEN BEHOEVE VAN ALGEMENE VOORWAARDEN

In sommige situaties is het sluiten van een Bewerkersovereenkomst niet noodzakelijk. In het kader van bouw-, installatie- en onderhoudswerkzaamheden worden Persoonsgegevens verwerkt. Het doel van de verwerking is echter niet het verwerken van die Persoonsgegevens an sich, het doel is het leveren van bouw-, installatie- en onderhoudswerkzaamheden. Voor het leveren van die dienst is het noodzakelijk om Persoonsgegevens, zoals een adres en naam, te verwerken. Zonder deze Persoonsgegevens zou het leveren van de dienst onmogelijk zijn. Het is dan echter niet noodzakelijk de verwerking van Persoonsgegevens op te nemen in een Bewerkersovereenkomst.

Wel is het belangrijk dat er zorgvuldig wordt omgegaan met de Persoonsgegevens. Om dit te bewerkstelligen is het aan te raden om bepalingen op te nemen in de algemene voorwaarden, Overeenkomst of inkoopvoorwaarden.

Hieronder is een overzicht van de standaardbepalingen die kunnen worden opgenomen die betrekking hebben op de verwerking van Persoonsgegevens.

**Algemene voorwaarden**

*Verwerking Persoonsgegevens*

1. Voor zover in het kader van het uitvoeren van de werkzaamheden Persoonsgegevens worden verwerkt, zullen deze Persoonsgegevens op een behoorlijke en zorgvuldige wijze worden verwerkt en overeenkomstig de Wet Bescherming Persoonsgegevens en Algemene Verordening Gegevensbescherming.

2. Technische en organisatorische maatregelen zullen worden getroffen om de Persoonsgegevens te beschermen tegen verlies of enige andere vorm van onrechtmatige verwerking, daarbij rekening houdend met de stand van de techniek en de aard van de verwerking.

**Inkoopvoorwaarden/Overeenkomst**

Wanneer ervoor wordt gekozen om afspraken over de verwerking van Persoonsgegevens op te nemen in de inkoopvoorwaarden/Overeenkomst, zorg dan dat ook de volgende definities worden opgenomen:

- Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de Betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
- Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
- Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte Persoonsgegevens betrekking hebben.
- Inbreuk in verband met Persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens (**'Datalek'**).
- Toezichthoudende autoriteit: een onafhankelijke overheidsinstantie verantwoordelijk voor het toezicht op de naleving van de wet in verband met de verwerking van Persoonsgegevens. In Nederland is dit de Autoriteit Persoonsgegevens.

*Verwerking Persoonsgegevens*

1. Wanneer de Opdrachtnemer tijdens het uitvoeren van de Overeenkomst Persoonsgegevens verwerkt, zal de Opdrachtnemer de Persoonsgegevens op een behoorlijke en zorgvuldige wijze verwerken en zich houden aan de wettelijke voorschriften die volgen uit de Wet Bescherming Persoonsgegevens en Algemene Verordening Gegevensbescherming.

2. De Opdrachtnemer informeert de Opdrachtgever binnen vier werkdagen over ieder verzoek en/ofiedere klacht van de Toezichthoudende autoriteit of de Betrokkene ten aanzien van de Persoonsgegevens die worden verwerkt bij het uitvoeren van de Overeenkomst.

3. De Opdrachtnemer verleent medewerking aan de Opdrachtgever wanneer de Betrokkene eenverzoek indient ter uitoefening van zijn of haar rechten zoals, maar niet beperkt tot, het recht op inzage, verbetering, verwijdering, bezwaar maken tegen de verwerking van de Persoonsgegevens en een verzoek tot overdraagbaarheid van de eigen Persoonsgegevens.

4. De Opdrachtnemer informeert de Opdrachtgever binnen vier werkdagen over ieder rechterlijk bevel, dagvaarding, wettelijke verplichting of anderszins verplichting tot het delen van Persoonsgegevens met derden.

5. De Opdrachtnemer informeert de Opdrachtgever over het ontdekken van een mogelijk Datalek binnen 24 uur na het ontdekken ervan. De Opdrachtnemer zal de Opdrachtgever vervolgens op de hoogte houden van nieuwe ontwikkelingen rondom het Datalek.

6. De Opdrachtnemer zal de volgende informatie verstrekken in geval van een Datalek:
   a. een gedetailleerde omschrijving van het Datalek;
   b. type/soort Persoonsgegevens betrokken bij het Datalek;
   c. van hoeveel personen de Persoonsgegevens betrokken zijn bij het Datalek;
   d. de identiteit van de personen betrokken bij het Datalek;
   e. de getroffen maatregelen om negatieve gevolgen voor de Betrokkenen te beperken en het Datalek te verhelpen;
   f. de oorzaak van het Datalek;
   g. de duur van het Datalek en het ontstaansmoment.

7. De eventuele kosten die gemaakt worden om het Datalek op te lossen, komen voor rekening van degene die de kosten maakt, tenzij het Datalek is ontstaan door het niet-nakomen van de Overeenkomst door de Opdrachtnemer, dan komen de kosten voor rekening van de Opdrachtnemer. Daarnaast behoudt de Opdrachtgever de mogelijkheid om andere rechtsmiddelen in te schakelen.

8. Communicatie over het Datalek zal altijd geschieden in overleg.

9. Wanneer de Overeenkomst tussen de Opdrachtnemer en Opdrachtgever eindigt, zal de Opdrachtnemer de Persoonsgegevens die hij heeft verwerkt bij het uitvoeren van de Overeenkomst teruggeven aan de Opdrachtgever en/of vernietigen.

Deze publicatie is een uitgave van Aedes vereniging van woningcorporaties, Bouwend Nederland en UNETO-VNI in samenwerking met Privacy Company.

**Tekst:** Diederik The, Arnold Roosendaal en Anouk Visser (Privacy Company)
**Vormgeving:** Aedes vereniging van woningcorporaties



vereniging van woningcorporaties
aedes
Bouwend Nederland
de vereniging van bouw- en infrabedrijven
UNETO-VNI
PRIVACY COMPANY