BEKNOPT OVERZICHT PERSOONSGEGEVENS BIJ BOUW, RENOVATIE EN ONDERHOUD

AANVULLING OP AEDES AVG-ROUTEPLANNER

vereniging van woningcorporaties

aedes

Bouwend Nederland

de vereniging van bouw- en infrabedrijven

Techniek Nederland

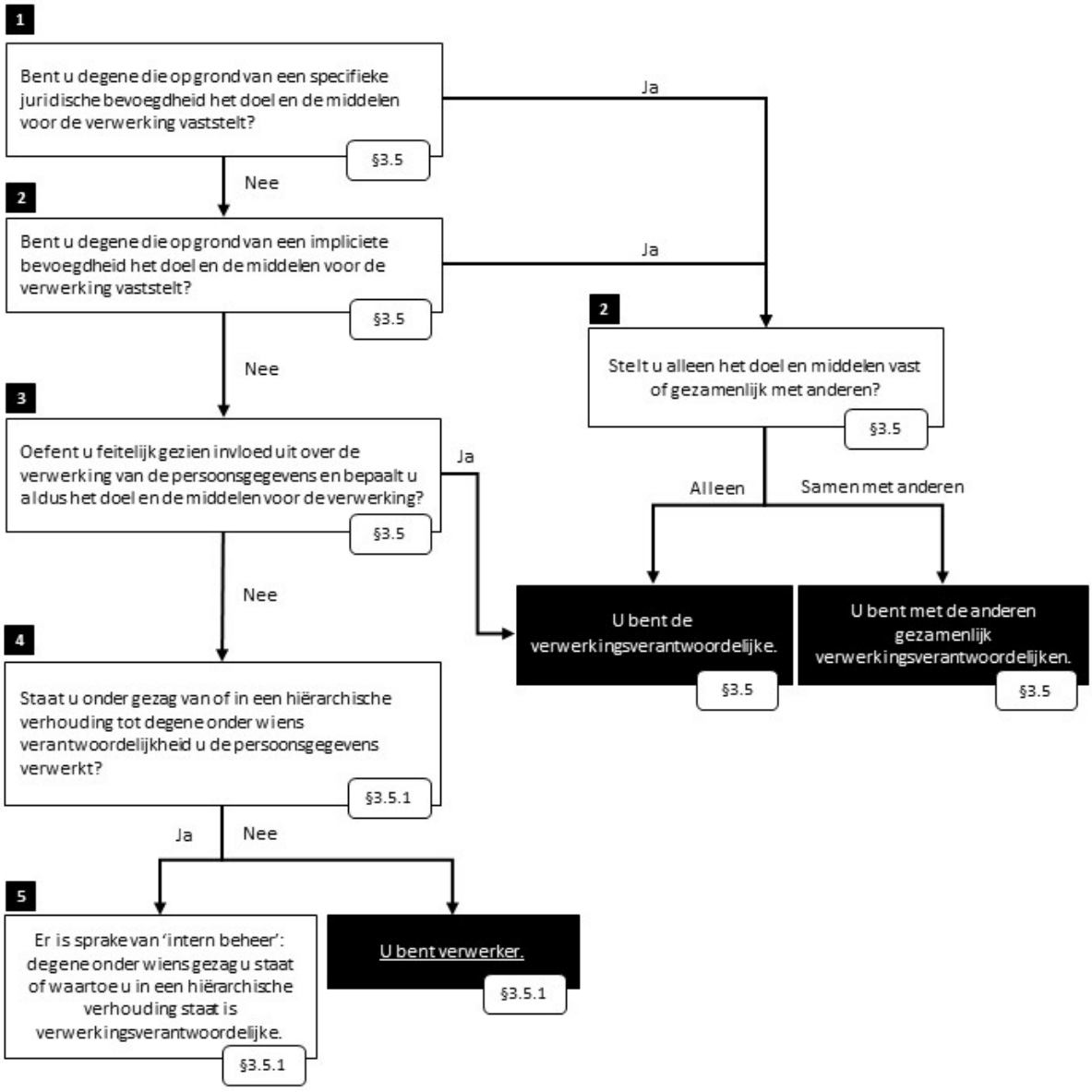
Inleiding

Als opdrachtgever (woningcorporatie) of opdrachtnemer (aannemer of installateur) heeft u veel te maken met het verwerken van persoonsgegevens. Denk hierbij aan het uitwisselen van adres- en contactgegevens tussen een woningcorporatie en aannemer of installateur. Het verwerken van persoonsgegevens is echter aan regels gebonden. De regels voor het verwerken van persoonsgegevens staan in de Algemene Verordening Gegevensbescherming (hierna AVG).

In de AVG staan twee partijen centraal als het gaat om het verwerken van persoonsgegevens te weten de *verwerkingsverantwoordelijke* en de *verwerker*. De komst van de AVG betekent meer rechten voor betrokkene maar ook meer verplichtingen voor organisaties. De verantwoordelijkheden die de AVG oplegt aan de verwerkingsverantwoordelijke en de verwerker nemen toe. In de praktijk is niet altijd helder hoe deze rolverdeling precies ligt, welke partij welke rol vervult: die van de verwerkingsverantwoordelijke of die van de verwerker?

Onderstaand schema uit de *Handleiding Algemene verordening gegevensbescherming* van de Autoriteit Persoonsgegevens (AP) geeft in algemene zin weer wanneer een partij verwerkingsverantwoordelijke of verwerker is.

Schema *Bent u een verwerkingsverantwoordelijke of verwerker?*



In het beknopte overzicht zal een duidelijk en pragmatisch overzicht worden geboden van de rolverdeling tussen de verwerkingsverantwoordelijke en de verwerker, en de verantwoordelijkheden die bij deze rollen komen kijken.

In dit document wordt de rolverdeling tussen verwerkingsverantwoordelijke en verwerker in een aantal veel voorkomende praktijksituaties weergegeven. Het overzicht dient als vervanging van de eerder door Aedes, Bouwend Nederland en Techniek Nederland opgestelde *Handreiking persoonsgegevens bij bouw, renovatie en onderhoud*. Hiermee zullen niet alle concrete gevallen in de praktijk zijn gedekt, maar het is een leidraad om aan de hand van deze voorbeelden in te kunnen schatten welke rol uw organisatie in het concrete praktijkgeval heeft.

Gangbare samenwerkingsvormen

In onderstaand overzicht zijn enkele gangbare samenwerkingsvormen tussen corporaties en aannemers/installateurs opgenomen. Per samenwerkingsvorm of situatie is aangegeven welke organisatie gezien moet worden als verwerker of verwerkingsverantwoordelijke. Per situatie is daarbij enige argumentatie opgenomen. Naast vier gangbare samenwerkingsvormen zijn er ook drie aanvullende varianten opgenomen die in combinatie met een samenwerkingsvorm kunnen voorkomen. Zie onderstaande kaders.

	Samenwerkingsvorm	De aannemer/ installateur is	De corporatie is	Argumentatie
1	Aannemer/installateur ontvangt van de corporatie een opdracht met contact- en adresgegevens om onderhoud uit te voeren. De aannemer/installateur verwerkt dit in eigen systemen en neemt zelf via de contactgegevens contact op met de bewoners om onderhoud in te plannen en/of om het onderhoud uit te voeren.	Verantwoordelijke	Verantwoordelijke	Het gaat in deze situatie om een verstrekking van persoonsgegevens. De aannemer/installateur is zelf verantwoordelijk voor het verwerken van de persoonsgegevens. Er hoeft voor dit deel dan ook geen verwerkers-overeenkomst te komen. Belangrijk uitgangspunt hierbij is: het doen van onderhoud is een taak van de woningcorporatie die zij uitbesteedt aan een aannemer/installateur. Het uitwisselen van persoonsgegevens is gericht op het uitvoeren van het onderhoud en niet op het verwerken van persoonsgegevens. Het verwerken van persoonsgegevens is dus een (noodzakelijke) bijkomstigheid. Zie paragraaf 3.5 Handleiding AVG van de Autoriteit Persoonsgegevens (AP): 'U verwerkt ten behoeve van de verwerkings-verantwoordelijke persoonsgegevens wanneer de verwerking van persoonsgegevens uw primaire opdracht is. Met andere woorden, uw dienst-

				verlening moet gericht zijn op het verwerken van persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke. Wanneer de verwerking van persoonsgegevens niet uw primaire opdracht is, maar het een uitvloeisel is van een andere vorm van dienstverlening, dan bent u als dienstverlener zélf de verwerkings-verantwoordelijke voor deze verwerking. Oftewel, het enkele feit dat u een opdracht krijgt van de verwerkingsverantwoordelijke is niet voldoende om te kunnen spreken van verwerkerschap, de opdracht moet gericht zijn op het verwerken van persoonsgegevens.'
2	De aannemer/installateur ontvangt vanuit de corporatie via een koppeling tussen het systeem van de corporatie en de aannemer/installateur gegevens over uit te voeren onderhoud incl. de benodigde persoonsgegevens (contact- en adresgegevens). Hij verwerkt de gegevens in het eigen systeem en gebruikt deze gegevens om contact te leggen met de bewoner om het onderhoud uit te voeren.	Verantwoordelijke	Verantwoordelijke	Het gaat in deze situatie om een verstrekking van persoonsgegevens. De aannemer/installateur is zelf verantwoordelijk voor het verwerken van de persoonsgegevens. Er hoeft voor dit deel dan ook geen verwerkers-overeenkomst te komen. Ondanks dat de persoonsgegevens via een koppeling worden uitgewisseld is deze situatie feitelijk gezien niet anders dan samenwerkingsvorm 1. Het bij samenwerkingsvorm 1 genoemde uitganspunt en de vermelde toelichting uit de Handleiding AVG zijn ook van toepassing.
3	Aannemer/installateur werkt in het systeem van de corporatie. De aannemer/installateur kan inloggen en verwerkt de gegevens over het uit te voeren onderhoud incl. de benodigde persoonsgegevens van	Gezamenlijke verantwoordelijke	Gezamenlijke verantwoordelijke	De corporatie en aannemer/installateur zijn gezamenlijk verantwoordelijk voor het deel waar ze in samenwerken. Beide partijen hebben een bepalende rol bij het vaststellen van het doel en

	de bewoners (contact- en adresgegevens). De persoonsgegevens gebruikt hij om contact te leggen met de bewoners om het onderhoud uit te voeren.			de middelen bij de verwerking van persoons-gegevens binnen het systeem. Zowel de corporatie als de aannemer bepalen het doel van de verwerking in het gezamenlijk systeem. Waarschijnlijk heeft de corporatie wel zelf de werking van het systeem bepaald en heeft hij dit ook zonder de aannemer ontwikkeld. Dit neemt niet weg dat beide partijen wel iets te zeggen hebben over bijvoorbeeld de wijze van invoer, opslag, aanpassing van gegevens in het systeem. Er is dus een mate van gezamenlijkheid in het bepalen van het doel en de middelen bij verwerkingen binnen één systeem. Omdat ze in hetzelfde systeem samenwerken, is het raadzaam om onderling afspraken te maken over verantwoordelijkheden en de verdeling van de aansprakelijkheid. Zie pagina 33 Handleiding AVG van de Autoriteit Persoonsgegevens (AP): 'Wanneer de verantwoordelijke samen met anderen doel en middelen bepaalt, dan is er sprake van gezamenlijke verantwoordelijkheid. Dit is bijvoorbeeld het geval als een computer-fabrikant en een fitnessbedrijf samen een smartwatch ontwikkelen die gezondheidsgegevens registreert en de beide partijen gezamenlijk bepalen hoe en waarom deze gezondheids-gegevens worden verwerkt.

				Bij gezamenlijke verantwoordelijkheid moeten de partijen onderling duidelijke afspraken maken over wie invulling geeft aan de diverse rechten en plichten uit de Verordening. Het is met name van belang dat de betrokkene weet waar hij terecht kan om zijn rechten uit te oefenen. Ongeacht de afspraken tussen de gezamenlijke verwerkings-verantwoordelijken blijven zij hoofdelijk aansprakelijk voor de naleving van de Verordening.'
4	Bewoners van de corporatie kunnen rechtstreeks contact opnemen met de aannemer/installateur indien onderhoud nodig is. Om de bewoners van de corporatie tot dienst te kunnen zijn heeft de aannemer/installateur de contact- en adresgegevens van alle bewoners opgenomen in zijn eigen systemen.	Verantwoordelijke	Verantwoordelijke	Persoonsgegevens worden eenmalig verstrekt en overgenomen in het systeem van de aannemer/ installateur. De aannemer/installateur is in deze situatie zelf verantwoordelijk voor de verwerking van de persoonsgegevens. Belangrijk uitgangspunt hierbij is: het doen van onderhoud en het ontvangen van verzoeken hiertoe is een taak van de woningcorporatie die zij uitbesteed aan een aannemer/installateur. Naast het uitvoeren van het onderhoud is in deze situatie ook het ontvangen van verzoeken tot onderhoud uitbesteed. Het gebruik en de uitwisseling van persoonsgegevens is gericht op het uitvoeren van het onderhoud en niet op het verwerken van persoonsgegevens. Het verwerken van persoonsgegevens is dus een (noodzakelijke) bijkomstigheid. Het bij samenwerkingsvorm 1 genoemde uitgangspunt en de vermelde toelichting uit de Handleiding AVG zijn ook van toepassing.

In alle gevallen is de aannemer/installateur verantwoordelijke. De belangrijkste reden hiervoor is dat het verwerken van de persoonsgegevens niet het doel is van de opdracht maar het uitvoeren van onderhoud. Het verwerken van persoonsgegevens is een uitvloeisel van de gevraagde dienstverlening, namelijk het uitvoeren van onderhoud.

Varianten op de gangbare samenwerkingsvormen

	Samenwerkingsvorm	De aannemer/ installateur is	De corporatie is	Argumentatie
A	De aannemer/installateur gebruikt de contact-gegevens naast het uitvoeren van onderhoud ook om tevredenheidsenquêtes uit te voeren om inzicht te krijgen in de kwaliteit van het eigen werk.	Verantwoordelijke	-	Het gaat bij deze variant om een verdere verwerking voor eigen doeleinden van de aannemer/installateur. De aannemer/installateur is verantwoordelijke voor de verwerking van de persoonsgegevens voor eigen doeleinden. De corporatie heeft verder geen rol meer bij deze verwerking. Let op! Deze variant komt minder vaak voor. Vaak neemt de corporatie (als opdrachtgever) tevreden-heidsenquêtes af in plaats van dat de aannemer/ installateur dit zelf uitvoert.
B	De aannemer/installateur voert niet alle werkzaam-heden zelf uit maar schakelt een onderaannemer/ installateur in. De aannemer/installateur deelt daarvoor de contact- en adresgegevens van de bewoners met de onderaannemer/installateur.	Verantwoordelijke	-	De onderaannemer/installateur is in deze situatie zelf verantwoordelijk voor de verwerking van de persoonsgegevens die hij van de aannemer/ installateur ontvangt. Het verwerken van de persoonsgegevens door de onderaannemer/ installateur is namelijk geen primaire taak maar enkel een (noodzakelijke) bijkomstigheid.
C	In sommige gevallen komt deze aannemers/ installateur er achter dat bepaalde contactgegevens niet kloppen (denk aan onjuiste of ontbrekende telefoonnummer en/of e-mailadressen) en komen zij in contact met de huurders aan de juiste gegevens. Op verzoek van de corporaties worden deze gegevens	Verantwoordelijke	Verantwoordelijke	In deze situatie blijven beide partijen verantwoordelijk. De aannemer krijgt contact-gegevens van de woningcorporatie om ervoor te kunnen zorgen dat er onderhoud gepleegd wordt bij de woningen. De primaire opdracht is niet gericht op het verwerken van persoonsgegevens, maar een uitvloeisel van de onderhoudswerkzaamheden. De

	teruggekoppeld vanuit de aannemer/installateur naar de corporatie.			contactgegevens heeft de aannemer in eigen beheer. De aannemer zorgt ervoor dat zijn database up-to-date blijft door de contactgegevens die niet kloppen aan te passen. Op verzoek van de woningcorporatie stuurt de aannemer de aan-gepaste contactgegevens aan de woningcorporatie, zodat ook de woningcorporatie de database up-to-date heeft. De database up-to-date houden doet de aannemer voor zichzelf en niet namens de woningcorporatie. Dit is een uitvloeisel van de onderhoudswerkzaamheden. Op verzoek van de woningcorporatie verstrekt de aannemer de aangepaste contactgegevens. In deze situatie is er sprake van een verstrekker – ontvanger situatie (verwerkingsverantwoordelijk – verwerkings-verantwoordelijke). Zie hierbij ook paragraaf 3.5 Handleiding AVG van de Autoriteit Persoonsgegevens (AP).

Enkele begrippen uitgewerkt

Verwerkingsverantwoordelijke

Op het moment dat persoonsgegevens worden verwerkt moet iemand in de zin van de wet voor dit gebruik aansprakelijk zijn. Anders kan een betrokkene (de persoon wiens persoonsgegevens door de organisatie worden verwerkt) nooit weten wie hij moet aanspreken als er een fout wordt gemaakt met zijn of haar persoonsgegevens, of wanneer de betrokkene bijvoorbeeld zijn recht op inzage wil inroepen. Deze juridisch aansprakelijke persoon of organisatie wordt de verwerkingsverantwoordelijke genoemd, wat inhoudt dat die persoon of organisatie letterlijk verantwoordelijk is voor het verwerken van persoonsgegevens en dat het aan die persoon of organisatie is om in overeenstemming met de AVG persoonsgegevens te verwerken. De definitie van verwerkingsverantwoordelijke volgt uit artikel 4 lid 7 van de AVG: '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.'

Verantwoordelijkheden van de verwerkingsverantwoordelijke[1]

Het is van belang om vast te stellen wie de verwerkingsverantwoordelijke voor een verwerking is, aangezien de verwerkingsverantwoordelijke degene is die moet zorgen dat de verwerking in overeenstemming met de wet plaatsvindt[2]. Op het moment dat een verwerking niet in overeenstemming met de AVG plaatsvindt, is de verwerkingsverantwoordelijke in ieder geval aansprakelijk en loopt deze het risico op aanzienlijke boetes. Het is daarom van groot belang dat een verwerkingsverantwoordelijke zich goed bewust is van zijn verantwoordelijkheden.

De verantwoordelijkheden van de verwerkingsverantwoordelijke worden op verscheidene plaatsen in de wet beschreven. Deze zullen hier kort worden opgesomd. De verwerkingsverantwoordelijke draagt er zorg voor dat de volgende belangrijke beginselen van verwerking van toepassing zijn als er persoonsgegevens worden verwerkt:

- Persoonsgegevens worden verwerkt op een wijze die ten aanzien van de betrokken rechtmatig, behoorlijk en transparant is[3].
- De verwerking vindt plaats op basis van een legitieme grondslag[4]. Grondslagen van verwerkingen worden opgesomd in artikel 6 van de AVG (zie ook kader hieronder).
- De verwerking en eventuele verdere verwerking van persoonsgegevens vindt slechts plaats op grond van welbepaalde, uitdrukkelijk omschreven, gerechtvaardigde doelen[5].
- Alleen die persoonsgegevens worden verwerkt die toereikend en ter zake dienend zijn en beperkt tot wat noodzakelijk is voor vastgestelde doeleinden[6].
- Persoonsgegevens worden langer verwerkt in een vorm die het mogelijk maakt om de betrokkene te kunnen identificeren als dit niet langer noodzakelijk is voor het te bereiken doel[7].

[1] Zie hoofdstuk 5 *Handleiding Algemene verordening gegevensbescherming* voor uitgebreide informatie over de verantwoordelijkheden.
[2] Artikel 24 lid 1 AVG.
[3] Artikel 5 lid 1 sub a AVG.
[4] Artikel 6 AVG.
[5] Artikel 5 lid 1 sub b AVG.
[6] Artikel 5 lid 1 sub c AVG.
[7] Artikel 5 lid 1 sub e AVG.

- Passende concrete technische en organisatorische beveiligingsmaatregelen worden genomen om de persoonsgegevens te beschermen[8]. Als de verwerkingsactiviteiten hiertoe aanleiding geven (bijvoorbeeld door schaal of door de gevoeligheid van gegevens) moet de verwerkingsverantwoordelijke onder de AVG een beveiligingsbeleid hebben[9].
- Voldaan wordt aan de aparte, strengere regimes voor de verwerking van bijzondere persoonsgegevens en gevoelige persoonsgegevens, waaronder wettelijke persoonsnummers en strafrechtelijke gegevens[10].
- De betrokkene zijn of haar rechten kan uitoefenen (hoofdstuk III AVG).
- Waar nodig moeten afspraken met verwerkers worden gemaakt over de verwerking van persoonsgegevens[11].
- Datalekken moeten bij de AP en indien nodig aan betrokkene worden gemeld[12].
- Een Functionaris voor de Gegevensbescherming (FG) wordt ingesteld als dit noodzakelijk is[13].
- De verwerkingsverantwoordelijke moet bij het ontwikkelen van (nieuwe) producten of diensten rekening houden met privacy by design en privacy by default[14].
- De verwerkingsverantwoordelijke moet er voor zorgen dat hij alleen een beroep doet op verwerkers 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[15].
- De verwerkingsverantwoordelijke moet een register bijhouden van alle verwerkingsactiviteiten met betrekking tot persoonsgegevens[16].
- De verwerkingsverantwoordelijke moet bij risicovolle verwerkingen, van tevoren, een Gegevensbeschermingseffectbeoordeling, ook wel bekend als een PIA, uitvoeren[17]. Of een verwerking risicovol is wordt bepaald aan de hand van de aard, de omvang, de context en de doeleinden van de verwerking[18].

Verwerker

De definitie van verwerker is te vinden in artikel 4 lid 8 van de AVG en luidt: 'verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.'

Verantwoordelijkheden van de verwerker[19]

De verwerker is primair gebonden aan de vereisten die verwerkingsverantwoordelijke aan de verwerking stelt. Deze verplichtingen worden opgenomen in een verwerkersovereenkomst. De verantwoordelijkheden van een verwerker zijn onder andere opgenomen in artikel 28 AVG.

---

[8] Artikel 5 lid 1 sub f en artikel 32 AVG.
[9] Artikel 24 lid 2 AVG.
[10] Artikel 9, 10 en 11 AVG.
[11] Artikel 28 AVG.
[12] Artikel33 en 34 AVG.
[13] Artikel 37 e.v. AVG.
[14] Artikel 25 AVG.
[15] Artikel 28 AVG.
[16] Artikel 30 AVG.
[17] Artikel 35 AVG.
[18] Wilt u hier meer over weten? Lees dan de richtsnoeren van de WP29 over het bepalen of er sprake is van een waarschijnlijk hoog risico.
[19] Zie hoofdstuk 6 *Handleiding Algemene verordening gegevensbescherming* voor uitgebreide informatie over de verantwoordelijkheden.

De verwerker draagt er zorg voor dat:

- sprake is van passende technische en organisatorische maatregelen om de persoonsgegevens te beschermen[20];
- geen gebruik wordt gemaakt van een andere (sub)verwerker zonder voorafgaande algemene of specifieke schriftelijke toestemming van de verwerkingsverantwoordelijke[21];
- goede procedures zijn ingericht om de verwerkingsverantwoordelijke te ondersteunen bij het behartigen van de rechten van betrokkenen[22];
- na voltooiing van de werkzaamheden die in opdracht van de verwerkingsverantwoordelijke worden verricht worden de betreffende persoonsgegevens teruggegeven of vernietigd[23]. Na voltooiing van de werkzaamheden die in opdracht van de verwerkingsverantwoordelijke worden verricht worden de betreffende persoonsgegevens teruggegeven of vernietigd[24];
- te allen tijde alle documentatie die nodig is om compliance aan te kunnen tonen aan de verwerkingsverantwoordelijke kan worden verstrekt[25];
- hij de verwerkingsverantwoordelijke onmiddellijk informeert op het moment dat hij van mening is dat diens instructies in strijd zijn met de wet[26];
- in ieder geval al het personeel dat met persoonsgegevens moet werken onderworpen is aan een geheimhoudingsplicht[27];
- een overzicht wordt bijgehouden van alle categorieën van verwerkingsactiviteiten die voor de verwerkingsverantwoordelijke worden uitgevoerd (Register van verwerkingsactiviteiten)[28]. Dit register bevat onder andere:
  - de naam en contactgegevens van de verwerkers en verwerkingsverantwoordelijken waarvoor de verwerker persoonsgegevens verwerkt
  - de categorieën van verwerkingen die voor elke verwerkingsverantwoordelijke 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[29];
- beveiligingsincidenten/datalekken zonder vertraging worden gemeld aan de verwerkingsverantwoordelijke[30];
- indien nodig een FG wordt aangesteld[31];
- bij grensoverschrijdende gegevensoverdracht naar derde landen de regels van de AVG in acht worden genomen[32].

[20] Artikel 28 lid 1, 3 sub e en 4, en artikel 32 AVG.
[21] Artikel 28 lid 2 en 4 AVG.
[22] Artikel 28 lid 3 sub e AVG.
[23] Artikel 28 lid 3 sub g AVG.
[24] Artikel 28 lid 3 sub g AVG.
[25] Artikel 28 lid 3 sub h AVG.
[26] Artikel 28 lid 3 sub h AVG.
[27] Artikel 28 lid 3 sub b AVG en artikel 29 AVG.
[28] Artikel 30 lid 2 AVG.
[29] Artikel 31 AVG.
[30] Artikel 33 lid 2 AVG.
[31] Artikel 37 AVG.
[32] Artikel 44 AVG.

Verwerkersovereenkomst

Een overeenkomst tussen een verwerkingsverantwoordelijke en een verwerker wordt een verwerkersovereenkomst genoemd. In een dergelijke overeenkomst worden de rechten en plichten die de verwerkingsverantwoordelijke en de verwerker over en weer hebben op een rij gezet. Het sluiten van een verwerkersovereenkomst is verplicht gesteld[33], waarvoor zowel verwerkingsverantwoordelijke als verwerker verantwoordelijk voor zijn. Het sluiten van een verwerkersovereenkomst is verplicht gesteld[34], waarvoor zowel verwerkingsverantwoordelijke als verwerker verantwoordelijk voor zijn. Hiermee regel je dat de verwerker zorgvuldig met de persoonsgegevens omgaat. Hierbij is de feitelijke situatie leidend.

Een verwerkersovereenkomst moet in ieder geval de volgende onderdelen bevatten[35]:
(de optionele maar wel aan te raden onderdelen zijn schuingedrukt)

- definiëring van begrippen;
- totstandkoming, duur en beëindiging van de overeenkomst;
- vaststelling van het soort persoonsgegevens dat verwerkt wordt;
- vaststelling van het doel van de verwerking;
- vaststelling van het soort verwerkingen, op instructie van de verwerkingsverantwoordelijke;
- beveiligingsmaatregelen;
- afspraken over de algemene of specifieke voorafgaande schriftelijke toestemming voor het inschakelen van subverwerkers;
- export van persoonsgegevens buiten de EU/EER;
- geheimhouding van persoonsgegevens;
- procedure met betrekking tot datalekken;
- dat de verwerker de verwerkingsverantwoordelijke ondersteunt bij het doen nakomen van de verplichtingen in hoofdstuk III AVG;
- bepaling omtrent teruggave van persoonsgegevens na afloop van de verwerkersovereenkomst en de bewaartermijn van persoonsgegevens;
- dat de verwerker de verwerkingsverantwoordelijke ondersteunt bij het aantonen van compliance;
- aansprakelijkheidsclausules indien er inbreuk wordt gemaakt op de afspraken in de verwerkersovereenkomst.

In bijlage 1 van deze handreiking is een modelverwerkersovereenkomst opgenomen. Deze modelverwerkersovereenkomst bevat de bovenstaande onderdelen en kan door uzelf worden aangevuld indien nodig.

Verwerkingsverantwoordelijkenovereenkomst

Een overeenkomst tussen twee verwerkingsverantwoordelijken wordt een verwerkingsverantwoordelijkenovereenkomst genoemd. Indien persoonsgegevens worden uitgewisseld tussen partijen zonder dat er sprake is van een verwerkingsverantwoordelijke aan de ene kant en een verwerker aan de andere kant, strekt het tot de aanbeveling om afspraken over de verantwoordelijkheid van deze gegevensuitwisseling op papier te zetten. In bijlage 2 is een model verwerkingsverantwoordelijkenovereenkomst opgenomen die in deze situatie gebruikt kan worden.

[33] Artikel 28 lid 3 AVG.
[34] Artikel 28 lid 3 AVG.
[35] Artikel 28 lid 3 AVG.

Bijlage 1
Modelverwerkersovereenkomst

Verwerkersovereenkomst [NAAM BEDRIJF]

Datum: [INVOEREN DATUM]

Contractpartijen:

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

hierna te noemen: **'Verwerkingsverantwoordelijke'**,

en

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

hierna te noemen: **'Verwerker'**,

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.
Verwerkingsverantwoordelijke hecht grote waarde aan het beschermen van deze Persoonsgegevens.
Om die reden leggen Partijen in deze Verwerkersovereenkomst 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 Verwerker 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 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 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 (**'Verwerkingsverantwoordelijke'**).

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 (**'Verwerker'**).

1.5 Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte Persoonsgegeven betrekking hebben.

1.6 Verwerkersovereenkomst: deze Overeenkomst inclusief de bijlagen (**'Verwerkersovereenkomst'**).

1.7 Overeenkomst: de hoofdovereenkomst waar deze Verwerkersovereenkomst 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 Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst treedt in werking op de datum waarop Partijen deze ondertekenen.

2.2 Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst en zal gelden voor zolang de Overeenkomst duurt.

2.3 Indien de Overeenkomst eindigt, eindigt deze Verwerkersovereenkomst automatisch; de Verwerkersovereenkomst kan niet apart worden opgezegd.

2.4 Na beëindiging van deze Verwerkersovereenkomst zullen de lopende verplichtingen voor Verwerker, zoals het melden van Datalekken waarbij Persoonsgegevens van Verwerkingsverantwoordelijke betrokken zijn en de plicht tot geheimhouding blijven voortduren.

3. Verwerken Persoonsgegevens

3.1 Verwerker verwerkt alleen Persoonsgegevens in opdracht van Verwerkingsverantwoordelijke en Verwerker heeft geen zeggenschap over de Persoonsgegevens. Verwerker volgt instructies van Verwerkingsverantwoordelijke ten aanzien van de verwerking op en mag de Persoonsgegevens niet op een andere manier verwerken, tenzij Verwerkingsverantwoordelijke Verwerker daar van tevoren toestemming of opdracht voor geeft.

3.2 In Bijlage 1 wordt opgenomen welke Persoonsgegevens Verwerker precies zal verwerken en voor welke verwerkingsdoeleinden.

3.3 Verwerker houdt zich aan de wet en verwerkt de gegevens op een behoorlijke, zorgvuldige en transparante wijze.

3.4 Verwerker mag zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke geen andere personen of organisaties inschakelen bij het verwerken van de Persoonsgegevens.
3.5 Wanneer Verwerker met toestemming van Verwerkingsverantwoordelijke andere organisaties inschakelt, moeten zij minimaal voldoen aan de eisen die zijn opgenomen in deze Verwerkersovereenkomst.
3.6 Wanneer Verwerkingsverantwoordelijke een verzoek van een Betrokkene ontvangt ten aanzien van het uitoefenen van zijn of haar rechten, dan werkt Verwerker 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 Verwerker zorgt ervoor dat de Persoonsgegevens voldoende worden beveiligd. Om verlies en onrechtmatige verwerkingen te voorkomen neemt Verwerker 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 Verwerker aan Verwerkingsverantwoordelijke ieder jaar een rapportage sturen waarin de genomen maatregelen staan en de eventuele aandachts- en/of verbeterpunten. Hiervoor brengt Verwerker geen kosten in rekening aan Verwerkingsverantwoordelijke.
4.4 Verwerkingsverantwoordelijke mag een audit laten uitvoeren om te bepalen of het verwerken van de Persoonsgegevens aan de wet en de afspraken uit deze Verwerkersovereenkomst voldoet. Verwerker 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 Verwerker komen wanneer blijkt dat Verwerker zich niet aan de verplichtingen in deze Verwerkersovereenkomst houdt.
4.6 De controle op de algehele verwerking van Persoonsgegevens door Verwerker kan, naast de auditmogelijkheid, ook geschieden via zelfevaluatie door Verwerker. Verwerker zal hierbij aan Verwerkingsverantwoordelijke een rapport verstrekken waarin Verwerker aantoont dat hij voldoet aan de wet en de afspraken uit deze Verwerkersovereenkomst. Deze rapportage dient te worden ondertekend door een directielid binnen de organisatie van Verwerker.
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 gemoeid met het wijzigen van de beveiligingsmaatregelen komen voor rekening van degene die de kosten maakt.

5. Exporteren Persoonsgegevens

5.1 Verwerker 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 Verwerkingsverantwoordelijke.

6. Geheimhouding

6.1 Verwerker zal de verstrekte Persoonsgegevens geheim houden, tenzij dit op basis van een wettelijke verplichting niet kan.

6.2 Verwerker 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 Verwerker Verwerkingsverantwoordelijke hierover informeren binnen een termijn van 24 uur overeenkomstig het proces volgend uit Bijlage 3, zodat Verwerkingsverantwoordelijke indien nodig een melding van het Datalek bij de Toezichthouder kan doen.

7.2 Verwerker zal Verwerkingsverantwoordelijke op de hoogte houden van nieuwe ontwikkelingen rondom het Datalek, ook zal Verwerker de getroffen maatregelen om het Datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen, overleggen aan Verwerkingsverantwoordelijke.

7.3 Verwerker mag geen melding van een Datalek aan de Toezichthouder doen, wanneer bij het Datalek Persoonsgegevens van Verwerkingsverantwoordelijke betrokken zijn. Ook mag Verwerker de Betrokkenen niet informeren over het Datalek. Deze verantwoordelijkheid ligt bij Verwerkingsverantwoordelijke.

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 Verwerker de verplichtingen uit deze Verwerkersovereenkomst niet nakomt, kan Verwerkingsverantwoordelijke Verwerker daarvoor aansprakelijk stellen.

8.2 Verwerker is aansprakelijk voor alle schade die Verwerkingsverantwoordelijke lijdt door het niet nakomen van de wet en de bepalingen uit deze Verwerkersovereenkomst, voor zover dit is ontstaan door de werkzaamheden van Verwerker.

8.3 *Indien Verwerker de verplichtingen in deze Verwerkersovereenkomst overtreedt, is Verwerker aan Verwerkingsverantwoordelijke een direct opeisbare boete verschuldigd van [BEDRAG] voor iedere overtreding en [BEDRAG] voor iedere dag dat Verwerker de overtreding begaat. Daarnaast behoudt Verwerkingsverantwoordelijke het recht om schadevergoeding te vorderen.* (optioneel)

8.4 Verwerker is aansprakelijk voor de aan Verwerkingsverantwoordelijke opgelegde bestuurlijke boete door de Toezichthouder als de schade het gevolg is van het onrechtmatig of nalatig handelen van Verwerker.

8.5 Verwerkingsverantwoordelijke is niet aansprakelijk voor aanspraken van Verwerker of andere personen en organisaties waar Verwerker de samenwerking mee is aangegaan of waarvan Verwerker Persoonsgegevens verwerkt, als dit het gevolg is van het onrechtmatig of nalatig handelen van Verwerker.

9. Teruggave Persoonsgegevens en bewaartermijn

9.1 Na het beëindigen van deze Verwerkersovereenkomst geeft Verwerker de Persoonsgegevens terug aan Verwerkingsverantwoordelijke.

9.2 De overgebleven Persoonsgegevens zal Verwerker vernietigen na verstrijken van de wettelijke bewaartermijn en/of op verzoek van Verwerkingsverantwoordelijke. Hierbij valt bijvoorbeeld te denken aan Persoonsgegevens die om belastingtechnische redenen bewaard moeten blijven.

9.3 Verwerker zal na de teruggave en/of vernietiging van de Persoonsgegevens schriftelijk aan Verwerkingsverantwoordelijke verklaren niet langer in het bezit te zijn van de Persoonsgegevens.

10. Slotbepalingen

10.1 Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst zijn daarom ook van toepassing op de Verwerkersovereenkomst.

10.2 Bij eventuele tegenstrijdigheden tussen de bepalingen in de Verwerkersovereenkomst en de Overeenkomst, gelden de bepalingen uit deze Verwerkersovereenkomst ten aanzien van de verwerking van Persoonsgegevens.

10.3 Afwijkingen van deze Verwerkersovereenkomst zijn slechts geldig wanneer Partijen dit samen schriftelijk afspreken.

Aldus door Partijen overeengekomen en ondertekend:

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

Verwerker:
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 Verwerkersovereenkomst 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 Verwerker:	
Verwerkingsdoelen:	
Verwerkingsverantwoordelijke:	
Verwerker:	
Sub-Verwerkers:	
Verwerkte Persoonsgegevens:	
Locatie verwerkingen:	
Bewaartermijn:	

Bijlage 2: Overzicht met beveiligingsmaatregelen

Overzicht van de beveiligingsnormen die de Verwerkingsverantwoordelijke aan de Verwerker 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 Verwerker namens de Verwerkingsverantwoordelijke 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.

Bijlage 2
Modelregeling verwerkingsverantwoordelijkenovereenkomst

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 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 gezamenlijk verantwoordelijk.
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

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 voorwelk 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:

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

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

Deze publicatie is een uitgave van Aedes vereniging van woningcorporaties, Bouwend Nederland en UNETO-VNI/Techniek Nederland.

Tekst: Ingrid Spanjaard (Techniek Nederland), Lidewij de Ruijter (Bouwend Nederland), Bas Buitendijk (Aedes vereniging van woningcorporaties, VVA-informatisering)
Vormgeving: Aedes vereniging van woningcorporaties

vereniging van woningcorporaties
aedes

Bouwend Nederland
de vereniging van bouw- en infrabedrijven

Techniek Nederland