Verwerkersovereenkomst

Onderdeel van de ACBIT, Algemene Corporatie Inkoopvoorwaarden bij IT

Mei 2024

Colofon

Redactie en vormgeving:

Aedes vereniging van woningcorporaties

Contact en meer informatie:

Gaby van der Peijl, adviseur opdrachtgeverschap & inkoop, g.vanderpeijl@aedes.nl, 06 351 124 59

Disclaimer

De verwerkersovereenkomst is een onderdeel van de ACBIT, de Algemene Corporatievoorwaarden bij IT. De ACBIT-toolbox bestaat uit onder andere: de ACBIT 2021 Inkoopvoorwaarden, een toelichting op de voorwaarden en een overeenkomstengenerator. De toolbox is met zorg en aandacht opgesteld. Er is geen garantie dat de informatie juist is op het moment waarop zij wordt ontvangen, of dat de informatie na verloop van tijd nog steeds juist is. De gebruikers van de toolbox zijn zelf verantwoordelijk voor de juiste toepassing en kunnen er geen rechten ontlenen aan de toolbox. Er wordt geen aansprakelijkheid aanvaard voor schade als gevolg van onjuistheden en/of gedateerde informatie.

Kopiëren, verspreiden en elk ander gebruik van de toolbox in geheel of in delen is toegestaan. De toolbox kan door de gebruiker worden gewijzigd, zonder enige voorafgaande mededeling.

Inhoud

INLEIDING

Het sjabloon verwerkersovereenkomst kan gebruikt worden om de verplichte overeenkomst tussen de rollen van verwerkingsverantwoordelijke en verwerker overeen te komen.

Het is belangrijk om onderscheid te maken tussen de rollen van verwerkingsverantwoordelijke, verwerker en gezamenlijk verwerkingsverantwoordelijke. Dit sjabloon kan gebruikt worden wanneer er sprake is van een verwerkingsverantwoordelijke en een verwerker. Dit is het geval wanneer de verwerkingsverantwoordelijke het doel en de middelen van de verwerking van persoonsgegevens bepaalt en hij de verwerker nodig heeft om deze verwerking te realiseren. Bijvoorbeeld een woningcorporatie die de salarisadministratie uitbesteedt. De partij die de salarisadministratie faciliteert, verwerkt de persoonsgegevens van de medewerkers van de woningcorporatie in opdracht van de woningcorporatie. Een ander voorbeeld is een woningcorporatie die voor het uitzetten van enquêtes een enquêtebureau inhuurt.

Daarnaast kan er ook sprake zijn van gezamenlijke verwerkingsverantwoordelijken of een zelfstandige verwerker. In die gevallen is dit sjabloon niet van toepassing.

Dit sjabloon is opgesteld met als uitgangspunt dat de verwerkersovereenkomst in aanvulling op een (raam)overeenkomst wordt gesloten. In de raamovereenkomst regelen de partijen een aantal algemene zaken.

Het is mogelijk dat de woningcorporatie op grond van de eerdere versies van dit document, overeenkomsten heeft afgesloten. Het sjabloon is aangepast aan de huidige terminologie en op basis van jurisprudentie. Aangezien deze aanpassing inhoudelijke wijzigingen kennen, is het raadzaam om reeds gesloten verwerkersovereenkomsten te vernieuwen. Bijvoorbeeld in het geval van aangescherpte vereisten voor overeenkomsten die voortvloeien uit de AVG.

Als de woningcorporatie inhoudelijk punten aanpast in deze verwerkersovereenkomst, bijvoorbeeld tijdens de onderhandelingen, dan is het aan te raden de aangepaste versie eerst ter controle te overleggen aan een jurist zodat beoordeeld kan worden of de verwerkersovereenkomst nog wel de essentiële punten bevat.

1. SJABLOON VERWERKERSOVEREENKOMST

Verwerkersovereenkomst [NAAM BEDRIJF]

Datum: [INVOEREN DATUM]

Contractpartijen:

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

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

en

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

1.4 Verwerkersovereenkomst: deze Overeenkomst inclusief de bijlagen ('Verwerkersovereenkomst').

1.5 Overeenkomst: de hoofdovereenkomst waar deze Verwerkersovereenkomst uit voortvloeit.

1.6 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').

1.7 Subverwerker: een verwerker die wordt ingeschakeld door Verwerker om (indirect) Persoonsgegevens te verwerken namens Verwerkingsverantwoordelijke.

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 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 of Verwerker hiertoe op grond van een Unierechtelijke of lidstatelijke bepaling verplicht is. In dit laatste geval stelt Verwerker Verwerkingsverantwoordelijke, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

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

3.3 Verwerker houdt zich aan de toepasselijke wet- en regelgeving voor de verwerking van persoonsgegevens, waaronder maar uitdrukkelijk niet beperkt tot de AVG en de Uitvoeringswet AVG, en verwerkt de gegevens op een behoorlijke, zorgvuldige en transparante wijze.

3.4 Verwerker mag een Subverwerker inschakelen die is gevestigd binnen de Europese Economische Ruimte (EER) en daarbinnen Persoonsgegevens zal verwerken, mits hij Verwerkingsverantwoordelijke hiervan schriftelijk in kennis heeft gesteld en Verwerkingsverantwoordelijke conform artikel 3.5 hierna geen bezwaar heeft gemaakt.

3.5 Verwerkingsverantwoordelijke kan, binnen dertig (30) dagen na de schriftelijke melding van Verwerker en onder opgaaf van redenen, bezwaar maken tegen het inschakelen, waaronder toevoegingen en vervangingen, van Subverwerkers zoals bedoeld in artikel 3.4 hierboven. In geval van een met redenen omkleed bezwaar treden Verwerker en Verwerkingsverantwoordelijke met elkaar in overleg over de inzet van de betreffende Subverwerker(s) ten behoeve van de uitvoering van de Overeenkomst en bijbehorende Verwerkersovereenkomst. Voor zover Partijen nog geen overeenstemming hebben bereikt, zal Verwerker de desbetreffende Subverwerker niet inschakelen.

3.6 Verwerker waarborgt contractueel en blijft ervoor verantwoordelijk dat alle door hem ingeschakelde Subverwerkers de verplichtingen ten aanzien van de Verwerking van Persoonsgegevens, zoals vervat in de Overeenkomst en deze Verwerkersovereenkomst, naleven, en met name, maar uitdrukkelijk niet beperkt tot, de verplichting afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen te bieden, om zo een passend beschermingsniveau van de Persoonsgegevens te waarborgen.

3.7 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.

3.8 Verwerker stelt de Verwerkingsverantwoordelijke onverwijld in kennis van elk verzoek dat hij van een Betrokkene ontvangt ten aanzien van de verwerking van Persoonsgegevens door Verwerker namens Verwerkingsverantwoordelijke. Verwerker antwoordt niet zelf op het verzoek, tenzij de Verwerkingsverantwoordelijke daartoe toestemming en/of opdracht heeft gegeven.

3.9 Indien het voor Verwerker niet direct duidelijk is of de Betrokkene een verzoek doet ten aanzien van de Persoonsgegevens die Verwerker namens Verwerkingsverantwoordelijke verwerkt, dan zal Verwerker de Betrokkene te kennen geven dat het verzoek aan de betreffende verwerkingsverantwoordelijke kan worden gericht, zonder te verwijzen naar of te communiceren over (de verwerking van Persoonsgegevens namens) Verwerkingsverantwoordelijke.

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 heeft één keer per jaar, of vaker indien daartoe een concrete en aantoonbare aanleiding bestaat, het recht de naleving van deze Verwerkersovereenkomst te (laten) controleren, bijvoorbeeld door middel van een audit. Verwerker verleent hierbij naar redelijkheid zijn medewerking en verstrekt hiertoe alle relevante informatie. Verwerker behoudt zich het recht voor om redelijke nadere eisen aan een audit te stellen die toezien op veiligheidsprocedures en om ervoor te waken dat zijn bedrijfsvoering niet onredelijk wordt verstoord.

4.5 De kosten van een audit, alsmede de voor de audit te maken (vooraf kenbaar gemaakte en door Verwerkingsverantwoordelijke schriftelijk geaccordeerde) arbeidskosten van Verwerker worden gedragen door Verwerkingsverantwoordelijke, tenzij uit de audit blijkt dat Verwerker zich niet aan de verplichtingen in deze Verwerkersovereenkomst houdt.

4.6 Indien Verwerker meent dat een instructie van Verwerkingsverantwoordelijke als bedoeld in artikel 4.4 van deze Verwerkersovereenkomst, een inbreuk oplevert op geldende wet- en regelgeving, waaronder de AVG, stelt hij Verwerkingsverantwoordelijke hiervan onmiddellijk op de hoogte.

4.7 De controle op de naleving van deze Verwerkersovereenkomst door Verwerker zoals bedoeld in artikel 4.4 hiervoor, kan, naar keuze van de Verwerkingsverantwoordelijke, ook geschieden via zelfevaluatie door Verwerker. De zelfevaluatie houdt in dat de Verwerkingsverantwoordelijke aan Verwerker een vragenlijst verstrekt. Verwerker vult de vragenlijst tijdig, volledig en naar waarheid in. Indien passend verstrekt Verwerker de nodige informatie en documentatie, zoals certificaten en rapportages, om de beantwoording van de vragenlijst te onderbouwen. Indien de beantwoording van de vragenlijst naar mening van Verwerkingsverantwoordelijke onvoldoende aantoont dat Verwerker conform deze Verwerkersovereenkomst persoonsgegevens verwerkt, dan is Verwerkingsverantwoordelijke gerechtigd als nog een (volledige) audit uit te voeren.

4.8 Indien uit de controle blijkt dat de door Verwerker getroffen maatregelen en voorzieningen niet in voldoende mate voldoen aan deze Verwerkersovereenkomst en/of de AVG, dan zal Verwerker onverwijld de nodige maatregelen treffen om hier alsnog aan te voldoen. Verwerker houdt Verwerkingsverantwoordelijke, al dan niet op verzoek, op de hoogte over de maatregelen die hij neemt en de implementatie daarvan.

4.9 Wanneer Verwerkingsverantwoordelijke vaststelt 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.

5.2 Indien Verwerker conform dit artikel 5 toestemming verkrijgt om persoonsgegevens buiten de EER te (laten) verwerken, dan doet hij dit alleen indien de Europese Commissie conform het beschermingsniveau voor dat land en de betreffende doorgifte adequaat heeft verklaard of Verwerker passende waarborgen biedt en de betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken.

5.3 Indien Verwerkingsverantwoordelijke Persoonsgegevens doorgeeft naar Verwerker buiten de EER en voor dit land geen adequaatheidsbesluit geldt, komen Verwerkingsverantwoordelijke en Verwerker de Standard Contractual Clauses van de Europese Commissie (C/2021/3972), met indien wenselijk daarin opgenomen extra waarborgen, overeen. Deze Standard Contractual Clauses, inclusief de bijbehorend Data Transfer Impact Assesment (DTIA) worden dan opgenomen als Bijlage bij deze Verwerkersovereenkomst.

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 Verwerker is aansprakelijk voor alle schade die Verwerkingsverantwoordelijke lijdt door het niet nakomen van de wet en/of de bepalingen uit deze Verwerkersovereenkomst, voor zover de schade is ontstaan door enig handelen of nalaten van Verwerker. De totale aansprakelijkheid van Verwerker, behalve voor schade van Betrokkenen, zal per gebeurtenis nooit meer bedragen dan:

a. hetgeen de verzekeraar van Verwerker uitkeert; of

b. indien Verwerker niet is verzekerd dan wel indien de verzekeraar niet of slechts een deel van de schade van Verwerkingsverantwoordelijke uitkeert, een bedrag van EUR 100.000,00.

8.2 Verwerker zal een deugdelijke beroepsaansprakelijkheidsverzekering en/of cybersecurity verzekering afsluiten die incidenten met betrekking tot de verwerking van Persoonsgegevens dekt. Op verzoek van Verwerkingsverantwoordelijke zal Verwerker een actueel certificaat van de verzekering(en) doen toekomen.

8.3 Indien Verwerker de verplichtingen uit deze Verwerkersovereenkomst niet nakomt, zal Verwerkingsverantwoordelijke Verwerker hier schriftelijk op aanspreken. Verwerkingsverantwoordelijke geeft Verwerker hierbij, afhankelijk van de aard van de overtreding, een redelijke termijn om de overtreding op te heffen. Als Verwerker na afloop van deze termijn de verplichtingen uit deze Verwerkersovereenkomst nog steeds niet nakomt, is Verwerker aan Verwerkingsverantwoordelijke, zonder dat enige ingebrekestelling of gerechtelijke tussenkomst vereist is, een direct opeisbare boete verschuldigd van € 2.500,- (zegge: tweeduizend vijfhonderd euro) voor iedere overtreding en € 500,- (zegge: vijfhonderd euro) voor iedere dag dat Verwerker de overtreding na afloop van de gegeven termijn laat voortduren, met een maximum van EUR 10.000,00 (zegge: tienduizend euro). Daarnaast behoudt Verwerkingsverantwoordelijke het recht om schadevergoeding en nakoming te vorderen. Deze boete strekt ter aansporing van Verwerker om deze Verwerkersovereenkomst na te komen en daarom wordt uitdrukkelijk beoogd om deze niet vatbaar te maken voor matiging op welke grond dan ook.

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

8.5 Verwerkingsverantwoordelijke is niet aansprakelijk voor aanspraken van Betrokkenen 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 De Verwerker houdt zich gedurende de looptijd van de Overeenkomst aan de bewaartermijnen die Verwerker en Verwerkingsverantwoordelijke zijn overeengekomen in Bijlage 1 bij deze Verwerkersovereenkomst en verwijdert Persoonsgegevens op verzoek van Verwerkingsverantwoordelijke, tenzij Verwerker wettelijk verplicht is de Persoonsgegevens te bewaren.

9.2 Bij het eindigen van deze Verwerkersovereenkomst zal Verwerker op eigen kosten, op verzoek en ter keuze van Verwerkingsverantwoordelijke binnen een redelijke termijn alle Persoonsgegevens aan Verwerkingsverantwoordelijke (i) ter beschikking stellen in een in overleg met Verwerkingsverantwoordelijke te bepalen gangbaar formaat en vervolgens alle bestaande kopieën wissen of (ii) alle Persoonsgegevens wissen, tenzij opslag voor Verwerker verplicht is op grond van een wettelijke verplichting.

9.3 Verwerker zal na de teruggave en/of vernietiging op verzoek van de Verwerker van de Persoonsgegevens schriftelijk aan Verwerkingsverantwoordelijke verklaren niet langer in het bezit te zijn van de Persoonsgegevens en/of in voorkomend geval verklaren op grond van welke wet en ten aanzien van welke Persoonsgegevens hij verplicht is tot opslag.

9.4 Verwerker is eveneens verantwoordelijk voor een gelijke naleving van dit artikel 9 door eventuele sub-verwerkers.

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:

2. BIJLAGEN

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.

<table>
<tr><td>Voor welke specifieke diensten heeft de verwerker persoonsgegevens nodig?</td><td colspan="3">Geef in onderstaande lijst de dienst aan die van toepassing is:
☐ Het uitvoeren van reparatie- of onderhoudswerkzaamheden
☐ Anders, namelijk …</td></tr>
<tr><td>Geef aan waarom de verwerker de persoonsgegevens nodig heeft</td><td colspan="3">De (sub)verwerker heeft de persoonsgegevens nodig voor de volgende werkzaamheden (aard en doeleinde):

☐ Het maken van afspraken (voorbeeld: voor reparatie- of onderhoudswerkzaamheden)
☐ Het sturen van een factuur
☐ Het hosten van een website
☐ Het leveren van een dienst aan de bewoner (voorbeeld: het monitoren van het energieverbruik)
☐ Anders, namelijk …</td></tr>
<tr><td rowspan="2">Autorisatie</td><td colspan="3">Aantal personen en bijbehorende functies die toegang hebben tot de gegevens bij verwerker:</td></tr>
<tr><td colspan="2">Aantal</td><td>Functie</td></tr>
<tr><td>Geef aan van wie de persoonsgegevens (categorieën betrokkenen) zijn en maak een inschatting van het aantal:</td><td colspan="3">☐ …… bewoners van [NAAM BEDRIJF]
☐ ……..medewerkers van [NAAM BEDRIJF]
☐ ……..anders, namelijk ……..</td></tr>
<tr><td>Geef aan welke persoonsgegevens van welke categorieën worden verwerkt, en voor welke periode</td><td>Persoonsgegevens

☐ Voornaam/ voornamen
☐ Achternaam</td><td>Categorie betrokkenen</td><td>Bewaartermijn</td></tr>
</table>

	☐ Huidige adresgegevens ☐ Email-adres(sen) ☐ Telefoonnummer ☐ Geslacht ☐ Geboortedatum ☐ Bankgegevens ☐ Inkomensgegevens ☐ Gegevens over gezinssamenstelling ☐ Kenmerknummer …… ☐ Bijzondere persoonsgegevens, namelijk … ☐ Anders, namelijk …		
Verwerkingsverantwoordelijke verleent conform artikel 3.4 toestemming aan Verwerker voor het laten uitvoeren van de volgende handelingen met persoonsgegevens door de volgende sub-verwerkers.	Sub-verwerker: Naam: Adres (incl. land): KvK-nummer (indien van toepassing): Soort dienst en specificatie van te verwerken persoonsgegevens: Verwerkersovereenkomst tussen Verwerker en Subverwerker: Ja/Nee Locatie van gegevensverwerking: Gegevens buiten de EER: Ja, het doorgifte mechanisme is […]/Nee		

	Aantal personen dat toegang heeft tot de gegevens:
	Sub-verwerker: Naam: Adres (incl. land): KvK-nummer (indien van toepassing): Soort dienst en specificatie van te verwerken persoonsgegevens: Verwerkersovereenkomst tussen Verwerker en Subverwerker: Ja/Nee Locatie van gegevensverwerking: Gegevens buiten de EER: Ja, het doorgifte mechanisme is […]/Nee
	Aantal personen dat toegang heeft tot de gegevens:
Geef de verschillende locaties aan waar de verwerkingen door de verwerker plaatsvinden (zowel voor opslag en verwerking van gegevens, als de back-up van gegevens):	

Bijlage 2: Overzicht met beveiligingsmaatregelen

Verwerker c.q. leverancier [NAAM VERWERKER] zal blijvend alle passende technische en organisatorische maatregelen nemen om de persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Verwerker zal zich overigens steeds houden aan de voor hem geldende verplichtingen ingevolge de AVG en de systemen technisch beheren en onderhouden.
Om vast te stellen wat passende beveiligingsmaatregelen zijn, moet door de Verwerker 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.

Verwerker is verplicht de verwerkte persoonsgegevens strikt gescheiden te houden van andere (persoons)gegevens (van derden en/of zichzelf).

Om te bepalen wat passende beveiligingsmaatregelen zijn, wordt een risicoafweging gemaakt op onder andere de volgende punten:

Om welk **type persoonsgegevens** gaat het?

☐ A. Gewone persoonsgegevens, zoals: NAW-gegevens, email-adressen, telefoonnummers, geslacht en/of geboortedatum;

☐ B. Bijzondere of gevoelige persoonsgegevens: zoals strafrechtelijk verleden, etnische afkomst, politieke opvattingen, BSN, gezondheid, biometrie en/of religieuze overtuigingen.

Indien er handelingen worden verricht met bijzondere persoonsgegevens, is er sprake van een verhoogd risicoprofiel. Deze bijzondere persoonsgegevens kunnen de privacy van een persoon namelijk ernstig beïnvloeden.

Hoeveel personen zijn betrokken bij de handelingen die de leverancier gaat uitvoeren met de persoonsgegevens?

☐ A. 50 tot 100 personen

☐ B. 100 tot 500 personen

☐ C. 500 tot 1500 personen

☐ D. 1500+ personen

Hoe meer personen betrokken zijn, hoe meer eisen gesteld worden aan de beveiliging van de persoonsgegevens.

Hoe langer de persoonsgegevens bewaard moet worden, hoe essentiëler het gebruik van strenge beveiligingseisen (voorbeelden: het toepassen van encryptie, het toepassen van Multi Factor Authenticatie en/of het gebruik van pseudoniemen).

Vink in onderstaande lijst aan welke beveiligingsmaatregelen gebruikt worden om de persoonsgegevens te beschermen:

☐ Certificering ISO 27001, NEN 7510 en/of vergelijkbaar, namelijk …
☐ Versleuteling
☐ Anonimisering
☐ Pseudonimisering
☐ Multi Factor Authenticatie
☐ Single Sign On
☐ Anders, namelijk ……

Geef een toelichting op de genomen beveiligingsmaatregelen:

……
……
……

Beveiligingsmaatregelen vanuit [NAAM BEDRIJF]

Om persoonsgegevens van onze bewoners met een passend niveau te beschermen, neemt [NAAM BEDRIJF] de Baseline Informatiebeveiliging woningcorporaties (BIC) versie X.X als uitgangspunt.

Er wordt onder andere gebruik gemaakt van Single Sign On voor de IT-systemen van [NAAM BEDRIJF]. Met Single Sign On worden gebruikers in de gelegenheid gesteld om eenmalig in te loggen, waarna automatisch toegang tot één of meerdere applicaties wordt verschaft. Afhankelijk van de persoonsgegevens die worden verwerkt, wordt Multi Factor Authenticatie gebruikt. Hierbij dient een gebruiker twee stappen te doorlopen om toegang te krijgen tot een applicatie.

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 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]:

Contactpersoon [NAAM BEDRIJF]

Bij twijfel of bij het ontdekken van een beveiligingsprobleem, neem contact op met de voor deze overeenkomst aan u toegewezen contactpersoon van naam bedrijf.

Toegewezen contactpersoon: <CONTACTPERSOON>

Telefoonnummer: <TELEFOONNUMMER>

e-mailadres: <EMAILADRES>

Geef in je e-mail beantwoording op de onderstaande vragen

Wij willen graag dat je de onderstaande vragen beantwoordt. Deze vragen zijn gelijk aan de informatie die aan de Autoriteit Persoonsgegevens moet worden verstrekt.

1. Uw contactgegevens
2. De van toepassing zijnde verwerkersovereenkomst
3. Datum/ tijd van incident
4. Geef een omschrijving van het incident
5. Geef aan waar het incident heeft plaatsgevonden
6. Geef aan of er sprake is van verlies of diefstal?
   a. Zo ja: Wat heb je verloren/ is gestolen?
   b. Zo ja: Is er aangifte gedaan bij de politie? (aangifte toevoegen)
7. Geef aan of er mogelijk gegevens gelekt of verloren gegaan?
   a. Zo ja: Van wie zijn er gegevens gelekt/verloren?
   b. Zo ja: Welke gegevens zijn er gelekt/verloren?
8. Om een volledig beeld van het probleem te creëren, dient bewijsmateriaal zoals screenshots, mailtjes meegezonden te worden.