AVG Routeplanner
Verwerkersovereenkomst

vereniging van woningcorporaties

aedes

Inleiding
Aedes wil haar leden ondersteunen bij de implementatie van de privacywetgeving. Daarvoor biedt zij onder andere de AVG Routeplanner voor woningcorporaties aan. De Routeplanner is ontwikkeld door Privacy Company. Het is een hulpmiddel voor woningcorporaties om zich voor te bereiden op de invoering van de Algemene Verordening Gegevensbescherming (AVG). Het ondersteunt bij het navigeren in de richting van compliance, doordat het inzicht geeft in de belangrijkste verplichtingen en concreet uitlegt wat gedaan moet worden om aan die verplichtingen te voldoen. Compliance is het begrip waarmee wordt aangeduid dat een persoon of organisatie werkt in overeenstemming met de geldende wet- en regelgeving.

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 bepaald 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. Voor informatie over hoe deze rollen en de bijbehorende verplichtingen worden gekwalificeerd verwijzen wij u naar het ‘Beknopt overzicht persoonsgegevens bij bouw, renovatie en onderhoud’. Daar vindt u daar de Modelregeling gezamenlijke verwerkingsverantwoordelijkheid en de Modelbepalingen privacy ten behoeve van algemene voorwaarden. Dit sjabloon is opgesteld met als uitgangspunt dat de verwerkersovereenkomst in aanvulling op een raamovereenkomst wordt gesloten. In de raamovereenkomst regelen de partijen een aantal algemene zaken. Een voorbeeld hiervan is geschilbeslechting.

Invulinstructie
Het is mogelijk dat de woningcorporatie op grond van de vorige versie van dit document, die volgt uit de ‘Handreiking persoonsgegevens bij bouw, renovatie en onderhoud’, overeenkomsten heeft afgesloten. Dit 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.
Indien een woningcorporatie werkt met een ander sjabloon voor het opstellen van een verwerkersovereenkomst, kunnen deze ook gebruikt worden. Let op de aangescherpte vereisten voor de overeenkomst 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.

AVG Routeplanner
Verwerkersovereenkomst

vereniging van woningcorporaties

aedes

INHOUD

Bijlagen

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'**,

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

Overwegende dat:

Partijen hebben op [DATUM] een Overeenkomst met betrekking tot [OMSCHRIJVING] gesloten met kenmerk [….]. Ter uitvoering van deze Overeenkomst worden Persoonsgegevens verwerkt. Verwerkingsverantwoordelijke stelt het doel en middelen vast voor de verwerking van persoonsgegevens conform artikel 4 lid 7 AV. Verwerker verwerkt ten behoeve van Verwerkingsverantwoordelijke Persoonsgegevens conform artikel 4 lid 8 AVG. Partijen hechten grote waarde aan het beschermen van deze Persoonsgegevens. Om die reden en conform artikel 28 lid 3 AVG 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
4. Risicotoets Privacy en Informatiebeveiliging en afgesproken maatregelen
5. Standard Contractual Clauses inclusief de door Partijen uitgevoerde data transfer impact assessment.

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, zoals bedoeld in artikel 28 lid 4 AVG.
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 buiten de EER, ook niet door Subverwerkers en/ of andere personen of organisaties, zonder daarvoor voorafgaande schriftelijke toestemming van de algemeen directeur 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 artikel 45 AVG het beschermingsniveau voor dat land en de betreffende doorgifte adequaat heeft verklaard of Verwerker conform artikel 46 AVG 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 5 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:

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 colspan="2">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 colspan="2">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="4">Aantal personen en bijbehorende functies die toegang hebben tot de gegevens bij verwerker:</td></tr>
<tr><td colspan="2">Aantal</td><td colspan="2">Functie</td></tr>
<tr><td colspan="2">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 colspan="2">Geef aan welke persoonsgegevens van welke categorieën worden verwerkt, en voor welke periode</td><td>Persoonsgegevens

☐ Voornaam/ voornamen
☐ Achternaam
☐ Huidige adresgegevens
☐ Email-adres(sen)
☐ Telefoonnummer
☐ Geslacht
☐ Geboortedatum
☐ Bankgegevens
☐ Inkomensgegevens
☐ Gegevens over gezinssamenstelling
☐ Kenmerknummer
……</td><td>Categorie betrokkenen</td><td>Bewaartermijn</td></tr>
</table>

	☐ 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. NAW-gegevens en email adressen
- 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.

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.

Voorbeelden van beveiligingsincidenten die gemeld moeten worden:

- Brieven of e-mails worden naar een verkeerd adres gestuurd.
- 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.
- 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:

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 Woonbedrijf.

Toegewezen contactpersoon: <CONTACTPERSOON>
Telefoonnummer: <TELEFOONNUMMER>
e-mailadres: <EMAILADRES>

Benodigde gegevens

Geef navolgende gegevens per e-mail door aan uw contactpersoon en aan [E-MAIL AVG VAN NAAM BEDRIJF].

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.

Contactpersoon <VERWERKER>

De contactgegevens van de privacy officer/ security officer, danwel de functionaris gegevensbescherming, waarmee Woonbedrijf contact opneemt bij vragen rondom de verwerking en de naleving van deze verwerkersovereenkomst:

Naam: <CONTACTPERSOON>
Telefoonnummer: <TELEFOONNUMMER>
e-mailadres: <EMAILADRES>

Bijlage 4: Risicotoets Privacy en Cybersecurity en afspraken rondom maatregelen

Verwerkingsverantwoordelijke heeft op <DATUM> een Risicotoets Privacy en Cybersecurity afgenomen rondom de in deze verwerkersovereenkomst omschreven diensten en het hieruit voortkomende gebruik van persoonsgegevens.
De ingevulde toets is als bijlage bijgevoegd. Partijen conformeren zich aan de afspraken zoals opgenomen in de rapportage.

Partijen spreken af binnen <AANTAL> maanden de toets te actualiseren.

Bijlage 5: Standard Contractual Clauses, inclusief Data Transfer Impact Assesment (SSC's+ DTIA)

STANDARD CONTRACTUAL CLAUSES

Module 2 - Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ( ) for the transfer of data to a third country.

(b) The Parties:
   i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
   ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

   have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
   i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
   ii. Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
   iii. Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
   iv. Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
   v. Clause 13;
   vi. Clause 15.1(c), (d) and (e);

vii. Clause 16(e);
viii. Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and 17rganizational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679**.**

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14€ to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible

adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ( ) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 30 days prior to the engagement of the sub-

processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ( ) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ( ) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
   i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
   ii. refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

~~[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.~~

~~[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.~~

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
   i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
   ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ( );
   iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
   i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
   ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
   i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
   ii. the data importer is in substantial or persistent breach of these Clauses; or
   iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

(d) In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(e) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(f) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

~~[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (specify Member State).]~~

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Netherlands (specify Member State).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used**.**