



Verwerkersovereenkomst

Veiligheidsregio Amsterdam-Amstelland



Voor u ligt de standaard voor een verwerkersovereenkomst van de Veiligheidsregio Amsterdam-Amstelland.

De Veiligheidsregio Amsterdam-Amstelland heeft de standaard voor een verwerkersovereenkomst "Standaard Verwerkersovereenkomst Gemeenten, versie 20 oktober 2020/ versie 2.3" van de VNG overgenomen en deels aangepast.



Verwerkersovereenkomst uitvoering <naam hoofdovereenkomst>

Veiligheidsregio Amsterdam-Amstelland, verder te noemen Verwerkingsverantwoordelijke, hierbij rechtsgeldig vertegenwoordigd door de <heer of mevrouw> <persoonsnaam>, <functie>

en

<Bedrijf>, gevestigd te <plaatsnaam>, KVK-nummer <nummer>, verder te noemen Verwerker, hierbij rechtsgeldig vertegenwoordigd door de <de heer of mevrouw>, <persoonsnaam>, <functie>,

hierna afzonderlijk te noemen "Partij", of gezamenlijk "Partijen"

Overwegen het volgende:

- a) Partijen hebben op <datum> de <titel hoofdovereenkomst>, hierna Hoofdovereenkomst, afgesloten, op grond waarvan Verwerker de volgende dienst(en) levert aan de Verwerkingsverantwoordelijke: <specificatie dienst(en)>;
- b) Verwerker verwerkt voor de uitvoering van de Hoofdovereenkomst Persoonsgegevens voor Verwerkingsverantwoordelijke;
- c) Op de verwerking van Persoonsgegevens door Verwerker zijn de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) van toepassing;
- d) Partijen willen in aanvulling op de AVG en de UAVG de volgende afspraken over de verwerking van Persoonsgegevens vastleggen in deze verwerkersovereenkomst (hierna: de Verwerkersovereenkomst);

En komen het volgende overeen:

Artikel 1 Definities

- 1.1 Begrippen uit de AVG en de UAVG die in deze Verwerkersovereenkomst worden gebruikt, hebben dezelfde betekenis.
- 1.2 Bijlagen: aanhangsels bij deze Verwerkersovereenkomst, die onlosmakelijk deel uitmaken van deze Verwerkersovereenkomst.
- 1.3 Toepasselijk Recht: de toepasselijke wet- of regelgeving, de Algemene Verordening Gegevensbescherming (EU) 2016/67 die per 25 mei 2018 van toepassing is of enige (andere) richtsnoeren, beleidsregels, instructies of aanbevelingen van enige bevoegde overheidsinstantie, van toepassing op de verwerking van de persoonsgegevens, daaronder begrepen enige wijzigingen, vervangingen, updates of andere latere versies daarvan.

Artikel 2 Ingangsdatum en duur

- 2.1 Deze Verwerkersovereenkomst gaat in op het moment dat de Hoofdovereenkomst tot stand is



gekomen, tenzij Partijen anders overeenkomen.

Artikel 3 Onderwerp van deze Verwerkersovereenkomst

- 3.1 Verwerker verwerkt de door of via Verwerkingsverantwoordelijke ter beschikking gestelde Persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke voor de uitvoering van de Hoofdovereenkomst en uitsluitend overeenkomstig schriftelijke instructies van Verwerkingsverantwoordelijke, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke wettelijke bepaling hem tot verwerking verplicht. In dat geval zal Verwerker Verwerkingsverantwoordelijke, voorafgaand aan de verwerking, daarvan zonder onredelijke vertraging in kennis stellen, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt. Verwerker heeft geen zelfstandige zeggenschap over de persoonsgegevens die door haar worden verwerkt. Verwerker zal de persoonsgegevens niet ten eigen nutte, ten nutte van derden, of voor andere doeleinden verwerken.
- 3.2 De door Verwerker uit te voeren verwerkingen staan beschreven in tabel 1 van Bijlage 1.



Artikel 4 Inhoudelijke afspraken

- 4.1 Verwerker zal geen persoonsgegevens overbrengen naar, toegankelijk maken vanuit of anderszins verwerken in een land buiten de Europese Economische Ruimte (EER), behoudens uitdrukkelijke schriftelijke toestemming van Verwerkingsverantwoordelijke.
- 4.2 Indien Verwerker voornemens is om persoonsgegevens buiten de EER te verwerken of anderszins naar een ander land buiten de EER door te geven (waaronder ook het toegankelijk maken van de persoonsgegevens vanuit (een entiteit in) een dergelijk ander land is begrepen), zal Verwerker – onverminderd het bepaalde in het eerste lid van dit artikel - Verwerkingsverantwoordelijke schriftelijk over dit voornemen informeren en daarbij tevens aangeven om welke land(en) het gaat.
- 4.3 Verwerker zal altijd en op eigen kosten haar volledige medewerking verlenen om te bewerkstelligen dat de eventuele doorgifte naar een land buiten de EER plaatsvindt in overeenstemming met het Toepasselijke Recht.
- 4.4 Personen die werken voor (sub)Verwerker en (sub)Verwerker zelf, moeten Persoonsgegevens waarmee zij werken geheimhouden. De personen die werken voor Verwerker en subverwerkers hebben daarom een geheimhoudingsverklaring getekend, of zich op een andere manier schriftelijk gebonden aan de geheimhouding.
- 4.5 Verwerker zal de Persoonsgegevens niet verstrekken aan derden, anders dan aan een door Verwerkingsverantwoordelijke vooraf goedgekeurde sub-verwerker, voor zover het betreft de Persoonsgegevens die nodig zijn voor een optimale dienstverlening door de sub-verwerker. De gegevens van een sub-verwerker worden opgenomen in tabel 3 van Bijlage 1. Bij de inschakeling van subverwerkers blijven de artikelen 28.2 en 28.4 AVG onverkort van kracht.
- 4.6 Verwerker zal met elke derde partij die zij inschakelt als sub-verwerker een schriftelijke sub-verwerkersovereenkomst sluiten en daarbij deze sub-verwerker dezelfde verplichtingen opleggen als die op haarzelf rusten uit hoofde van deze Verwerkersovereenkomst, daaronder begrepen maar niet beperkt tot de op haar rustende meldplichten inzake Datalekken. Verder zal Verwerker in deze sub-verwerkersovereenkomst de sub-verwerker verbieden om (sub-sub-)verwerkers in te schakelen, voor zover niet anders bepaald in de Overeenkomst.
- 4.7 Als een betrokkene een beroep doet op zijn rechten zoals genoemd in artikel 12 t/m 22 AVG, helpt Verwerker Verwerkingsverantwoordelijke om daarop binnen de wettelijke termijnen een beslissing te nemen.
- 4.8 Op verzoek van Verwerkingsverantwoordelijke werkt Verwerker altijd mee aan een gegevensbeschermingseffectbeoordeling (DPIA) en een voorafgaande raadpleging als bedoeld in artikel 35 en 36 AVG.

Artikel 5 Betrouwbaarheidseisen, Beveiliging en Audits

- 5.1 Verwerker zal tenminste de informatiebeveiligingseisen uit Bijlage 2 in acht nemen en de eveneens in Bijlage 2 uitgewerkte technische en organisatorische beveiligingsmaatregelen implementeren, opdat met deze maatregelen invulling wordt gegeven aan de betrouwbaarheidseisen zoals vastgesteld door Verwerkingsverantwoordelijke.
- 5.2 De door Verwerker te implementeren technische en organisatorische beveiligingsmaatregelen dienen een passend beschermingsniveau te verzekeren, onder meer met het oog op de verplichting van de Verwerkingsverantwoordelijke wat betreft het omgaan van verzoeken van betrokkenen die hun rechten uitoefenen. Dit in overeenstemming met het Toepasselijke Recht,



met inachtneming van de stand der techniek, de kosten gemoeid met de implementatie en aard, omvang, context en doeleinden van de verwerking, alsmede de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen. Deze maatregelen omvatten, waar passend, in ieder geval:

- a. pseudonimisering en versleuteling van de persoonsgegevens;
 - b. het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingsfaciliteiten en diensten te garanderen;
 - c. passende preventieve maatregelen, die Verwerker in staat stellen om een Datalek onmiddellijk te onderkennen en Verwerkingsverantwoordelijke tijdig daarover te informeren, zoals intrusion detection, toekomstbestendige versleuteling, de mogelijkheid om de beschikbaarheid van de persoonsgegevens tijdig te herstellen;
 - d. een proces voor het regelmatig testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische beveiligingsmaatregelen om de veiligheid van de verwerking van de persoonsgegevens te garanderen.
- 5.3 Bij de implementatie van enige beveiligingsmaatregel zal Verwerker het Toepasselijke Recht naleven.
- 5.4 Verwerker zal op regelmatige basis de getroffen technische en organisatorische beveiligingsmaatregelen evalueren en indien nodig actualiseren.
- 5.5 Tenzij Verwerker door middel van een geldige certificering, die periodiek door een geaccrediteerde instelling wordt getoetst, heeft aangetoond dat Verwerker de gemaakte afspraken nakomt, kan Verwerkingsverantwoordelijke de verwerkingsactiviteiten en de bewerkingsfaciliteiten, met inachtneming van een voorafgaande kennisgevingsperiode van 2 weken, (laten) onderwerpen aan een audit om de genomen technische en organisatorische maatregelen ter zake van de persoonsgegevens te (laten) onderzoeken.
- 5.6 Verwerkingsverantwoordelijke kan eveneens een audit (laten) uitvoeren ter zake van de verwerkingsactiviteiten en de bewerkingsfaciliteiten om te verifiëren of Verwerker Verwerkingsverantwoordelijke daadwerkelijk correct en tijdig ingelicht heeft over alle Datalekken, en de ter zake getroffen preventieve en herstelmaatregelen, daaronder begrepen enige maatregelen ter voorkoming van herhaling van een datalek.
- 5.7 Verwerker zal alle redelijkerwijs benodigde medewerking verlenen zodat Verwerkingsverantwoordelijke haar auditrechten kan uitoefenen en naleving van het Toepasselijke recht aan kan tonen, en Verwerker zal ervoor zorgen dat door haar ingeschakelde sub-verwerkers dit ook doen.
- 5.8 Verwerkingsverantwoordelijke kan derde partijen (experts) inschakelen voor de uitoefening van haar auditrechten. Het uitvoeren van een audit door Verwerkingsverantwoordelijke of namens Verwerkingsverantwoordelijke zal niet leiden tot vertraging van de werkzaamheden van Verwerker of een van haar Onderaannemers. Indien een dergelijke vertraging toch dreigt, zullen Partijen in overleg treden.
- 5.9 De kosten van audits worden gedragen door Verwerkingsverantwoordelijke (zowel eigen kosten als kosten van Verwerker), tenzij de auditor één of meer tekortkomingen van niet ondergeschikte aard van Verwerker constateert die ten nadele zijn van Verwerkingsverantwoordelijke.

Artikel 6 Inbreuk in verband met Persoonsgegevens



- 6.1 Verwerker zal Verwerkingsverantwoordelijke zonder onredelijke vertraging, maar uiterlijk binnen 24 uur, informeren na vaststelling van een (vermoedelijke) Inbreuk in verband met Persoonsgegevens zoals omschreven in Bijlage 3 van deze Verwerkersovereenkomst.
- 6.2 In geval van een Inbreuk neemt Verwerker zonder onredelijke vertraging alle maatregelen om de Inbreuk te herstellen, de gevolgen daarvan te beperken en verdere Inbreuken te voorkomen. Bovendien zal Verwerker Verwerkingsverantwoordelijke voorzien van alle door Verwerkingsverantwoordelijke verzochte relevante informatie met betrekking tot het datalek. Deze informatie omvat in ieder geval:
 - 6.2.1 een beschrijving van de aard en de omvang van het datalek, een inschatting van het aantal (mogelijk) getroffen betrokkenen en een indicatie van de aard van de getroffen persoonsgegevens en of deze persoonsgegevens versleuteld waren, dan wel anderszins beveiligd of onbegrijpelijk / ontoegankelijk waren gemaakt;
 - 6.2.2 een beschrijving van de getroffen en te treffen preventieve en correctieve maatregelen, geplande maatregelen en de aanbevolen maatregelen ter beperking van de schade en voorkoming van herhaling van het datalek, daaronder begrepen een noodplan en de verwachte oplossingstijd;
 - 6.2.3 informatie over welke derden, zoals particuliere personen en de (sociale) media, bekend zijn of kunnen zijn met het datalek;
 - 6.2.4 de contactgegevens van de bevoegde vertegenwoordiger(s) van Verwerker bij wie Verwerkingsverantwoordelijke onmiddellijk en regelmatig updates kan verkrijgen van de status van het datalek; en
 - 6.2.5 enige andere informatie die kan bijdragen aan de beperking van de schade aan de organisatie van Verwerkingsverantwoordelijke en de privacy van de getroffen betrokkene(n).
- 6.3 Verwerker heeft een gedetailleerd logboek van de Inbreuken en de maatregelen die op Inbreuken zijn genomen. Verwerkingsverantwoordelijke mag dat onverwijld inzien, wanneer deze daarom vraagt.
- 6.4 Verwerkingsverantwoordelijke beslist of de Inbreuk moet worden gemeld bij de toezichthoudende autoriteit en/of Betrokkene. Verwerker ondersteunt de Verwerkingsverantwoordelijke waar nodig bij de melding aan de toezichthoudende autoriteit en/of Betrokkene.

Artikel 7 Beëindigen verwerkersovereenkomst

- 7.1 Deze Verwerkersovereenkomst treedt in werking tegelijk met de inwerkingtreding van de Hoofdovereenkomst of, indien de Hoofdovereenkomst al van kracht is, vanaf het tijdstip van de ondertekening van deze Verwerkersovereenkomst door Partijen.
- 7.2 Deze Verwerkersovereenkomst zal van kracht zijn zolang de Hoofdovereenkomst van kracht is. Bij beëindiging van de Hoofdovereenkomst eindigt deze Verwerkersovereenkomst van rechtswege zonder dat enige nadere (rechts)handeling vereist is, evenwel met dien verstande dat zolang dat Verwerker nog niet alle persoonsgegevens aan Verwerkingsverantwoordelijke heeft geretourneerd respectievelijk verstrekt of deze heeft vernietigd en/of niet heeft voldaan aan het bepaalde in artikel 7.6, alle bepalingen in deze Verwerkersovereenkomst die naar hun aard voortduren, van kracht blijven totdat aan bedoelde retournering, verstrekking of vernietiging en het bepaalde in artikel 7.6 is voldaan.
- 7.3 Tussentijdse opzegging van deze Verwerkersovereenkomst door Verwerker is niet mogelijk.



- 7.4 Voor zover niet anders voortvloeit uit het Toepasselijke Recht, zal Verwerker, indien deze Verwerkersovereenkomst eindigt of op een eerdere datum zodra Verwerkingsverantwoordelijke aangeeft dat de verwerking van (een deel van) de persoonsgegevens niet langer ter zake dienend is voor de uitvoering van de diensten, ervoor zorgdragen: (i) dat de persoonsgegevens onmiddellijk op een door Verwerkingsverantwoordelijke geschikt bevonden wijze worden geretourneerd c.q. verstrekt aan Verwerkingsverantwoordelijke of aan een door Verwerkingsverantwoordelijke aangewezen vervangende dienstverlener, dan wel (ii) dat de persoonsgegevens onmiddellijk worden vernietigd, indien Verwerkingsverantwoordelijke daar schriftelijk om verzoekt.
- 7.5 Van de overdracht en de gevraagde vernietiging wordt door Verwerker een verslag gemaakt waarin wordt beschreven op welke wijze de gegevens onherstelbaar zijn vernietigd. Verwerkingsverantwoordelijke kan van de vernietiging een bewijs verlangen. De kosten van overdracht en vernietiging komen voor rekening van Verwerker.
- 7.6 Verwerker zal ervoor zorgdragen dat zij na retournering, verstrekking of vernietiging alle verwerkingen van (de betreffende) persoonsgegevens onmiddellijk staakt en gestaakt houdt. Verwerker zal Verwerkingsverantwoordelijke een schriftelijke bevestiging en garantie daarvan verlenen, en Verwerkingsverantwoordelijke toestaan om te verifiëren dat de (betreffende) persoonsgegevens niet langer worden verwerkt door Verwerker of een door haar ingeschakelde sub-verwerker.
- 7.7 Deze Verwerkersovereenkomst eindigt op het moment dat Verwerker de verwerking van Persoonsgegevens op grond van de Hoofdovereenkomst heeft beëindigd en de afspraken over het teruggeven en/of wissen van Persoonsgegevens zijn nagekomen.
- 7.8 De geheimhouding geldt ook nog na beëindiging van deze Verwerkersovereenkomst.

Artikel 8. Aansprakelijkheid en boetebepaling

- 8.1 Eventuele in de Hoofdovereenkomst overeengekomen beperkingen van de aansprakelijkheid hebben ook betrekking op de Verwerkersovereenkomst.
- 8.2 Indien Verwerker tekortschiet in de nakoming van de verplichtingen uit deze overeenkomst kan Verwerkingsverantwoordelijke hem in gebreke stellen. Ingebrekestelling geschiedt schriftelijk, waarbij aan Verwerker een redelijke termijn wordt gegund om alsnog zijn verplichtingen na te komen. Deze termijn is een fatale termijn. Indien nakoming binnen deze termijn uitblijft, is Verwerker in verzuim. Verwerker is onmiddellijk in verzuim als de nakoming van desbetreffende verplichting binnen de overeengekomen termijn reeds blijvend onmogelijk is.
- 8.3 Verwerker is aansprakelijk voor alle schade of nadeel voortvloeiende uit het niet-nakomen van, of in strijd handelen met de bij of krachtens de AVG gegeven voorschriften en/of het niet-nakomen van, of in strijd handelen met het in deze Verwerkersovereenkomst bepaalde, onverminderd de aanspraken op grond van wettelijke regels. Verwerker is aansprakelijk voor schade of nadeel voor zover ontstaan door zijn werkzaamheid, daaronder begrepen ontstane inbreuken op de persoonlijke levenssfeer van betrokkenen.
- 8.4 Verwerker vrijwaart Verwerkingsverantwoordelijke tegen aanspraken van derden, waaronder betrokkenen, in verband met het handelen van Verwerker in strijd met de Verwerkersovereenkomst, de AVG en/of andere regelgeving waarin eisen aan het verwerken van persoonsgegevens worden gesteld. Verwerker zal alle daarmee verband houdende en daaruit voortvloeiende kosten (waaronder mede begrepen kosten van juridische bijstand) en schade van de Verwerkingsverantwoordelijke vergoeden.



- 8.5 Indien Verwerker enige in deze Verwerkersovereenkomst neergelegde verplichtingen niet of niet-tijdig nakomt en de Autoriteit Persoonsgegevens Verwerkingsverantwoordelijke dientengevolge een (bestuurlijke) boete oplegt, is Verwerker hiervoor aansprakelijk en zal Verwerkingsverantwoordelijke een contractuele boete ter hoogte van hetzelfde bedrag opleggen aan Verwerker. Deze boete is zonder rechterlijke tussenkomst, ingebrekestelling of aanmaning direct opeisbaar. Deze boete is niet vatbaar voor verrekening. Oplegging van deze boete laat alle andere rechten en/of vorderingen van Verwerkingsverantwoordelijke (inclusief o.a. het recht op nakoming, schadevergoeding) onverlet.
- 8.6 Indien Verwerker zijn verplichtingen uit hoofde van artikel 4.4 (geheimhouding) of artikel 4.1 en 4.5 van deze Verwerkersovereenkomst (doorgifte van persoonsgegevens buiten de EER en inschakeling (sub)verwerkers) niet nakomt, zal deze onmiddellijk, zonder dat enige verdere actie of formaliteit is vereist, jegens de Verwerkingsverantwoordelijke een onmiddellijk opeisbare boete verbeuren ten bedrage van € 25.000,- (vijfentwintigduizend euro) voor iedere dergelijke inbreuk, zonder dat de Verwerkingsverantwoordelijke enig verlies of schade behoeft te bewijzen en onverminderd het recht van de Verwerkingsverantwoordelijke om aanvullende schadevergoeding te vorderen als daarvoor gronden zijn, behoudens rechterlijke matiging. De boete laat alle andere rechten of vorderingen, waaronder, doch niet uitsluitend, de vordering van Verwerkingsverantwoordelijke tot nakoming en het recht op schadevergoeding onverlet.

Artikel 9 Kosten

- 9.1 De met de uitvoering van deze Verwerkersovereenkomst gemoeide kosten zijn begrepen in de prijzen en vergoedingen zoals overeengekomen in deze Overeenkomst.

Artikel 10 Overige bepalingen

- 10.1 Op deze overeenkomst is Nederlands recht van toepassing. Alle geschillen, ook als alleen één Partij vindt dat er een geschil is, zullen in eerste instantie worden voorgelegd aan dezelfde bevoegde rechter als genoemd in de Hoofdovereenkomst.

Ondertekening

Aldus overeengekomen en in tweevoud ondertekend,

Ingangsdatum: <.....>

Veiligheidsregio Amsterdam-Amstelland

namens deze: <naam, functie>

<Naam organisatie>

namens deze: <naam, functie>



plaats: <.....>

plaats: <.....>

datum: <.....>

datum: <.....>



Bijlage 1: Overzicht van te verwerken persoonsgegevens

1. Naam verwerking, doeleinden categorieën van betrokkenen, categorieën persoonsgegevens en eventuele doorgifte naar derde landen.

Naam verwerking	Verwerkings-doeleinden	Categorieën van betrokkenen	Categorieën Persoonsgegevens (waaronder bijzondere persoonsgegevens)	Doorgifte naar derde landen	Bewaartermijn

2. Contactgegevens

Contactpersoon Verwerkingsverantwoordelijke (NB: Ook buiten kantooruren)	Naam: Contactgegevens:
Contactpersoon Verwerker (NB: Ook buiten kantooruren)	Naam: Contactgegevens:

NB: Eventuele wijzigingen in bovenstaande tabellen geven partijen op korte termijn aan elkaar door.

3. Ingeschakelde subverwerkers

Naam en contactgegevens subverwerker	KvK nummer	Uitbestede werkzaamheden	Doorgifte ja/nee	Indien ja, type passende waarborg



Bijlage 2: Passend niveau van beveiliging

Uitwerking van de basis technische en organisatorische maatregelen

Verwerker is gehouden de informatiebeveiliging van persoonsgegevens, die onder verantwoordelijkheid van Verwerkingsverantwoordelijke door Verwerker verwerkt worden, in te richten en de beveiligingsrisico's aantoonbaar te beheersen. Hiertoe behoren tenminste de ondergenoemde technische en organisatorische beveiligingsmaatregelen:

1. De door Verwerker ingerichte informatiebeveiliging bestaat uit een samenhangend geheel van organisatorische, procesmatige en technische maatregelen en de getroffen beveiligingsmaatregelen zijn in overeenstemming met de aard, de omvang, de context en het doel van de verwerking en met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten van betrokkenen, rekening houdend met de stand der techniek en het belang van Verwerkingsverantwoordelijke.
2. Verwerker zal Verwerkingsverantwoordelijke voorafgaand aan de sluiting van deze Verwerkersovereenkomst inzage verstrekken in het bij Verwerker geldende informatiebeveiligingsbeleid en de procedures die in dit kader worden gevolgd.
3. Verwerker heeft binnen haar eigen organisatie een functionaris aangewezen in de rol van Security Officer. Deze medewerker is voor Verwerkingsverantwoordelijke centraal aanspreekpunt bij potentiële beveiligingsrisico's en de coördinatie van ernstige beveiligingsincidenten in de dienstverlening. Deze functionaris is gemachtigd de noodzakelijke maatregelen te initiëren teneinde beveiligingsrisico's te reduceren tot een aanvaardbaar niveau.
4. Verwerker zal Verwerkingsverantwoordelijke informeren over de locatie van de data centers die Verwerker gebruikt in het kader van de uitvoering van de bovenliggende Overeenkomst en de diensten die zij uit hoofde van deze Overeenkomst aan Verwerkingsverantwoordelijke levert, alsmede de locatie van de data centers die Verwerker (eventueel) gebruikt als uitwijklocatie.
5. Verwerker beschikt over een adequaat en passend beleid inzake de back-up, restore en recovery van de voor de dienstverlening benodigde software en data en draagt zorg voor adequate fysieke bescherming van- en beheersing van de toegang tot de software en data in de back-up.
6. Verwerker heeft adequate fysieke en logische toegangsbeheersingsmaatregelen getroffen ter voorkomen van ongeautoriseerde toegang tot de persoonsgegevens.
7. Er wordt uitsluitend toegang verleend tot de persoonsgegevens aan personeel van Verwerker en door Verwerker ingehuurd personeel, verder "medewerkers" genoemd, en uitsluitend wanneer hier een legitieme noodzaak toe bestaat vanuit de in de Overeenkomst beschreven dienstverlening en de functieomschrijving van medewerkers.
8. Fysieke en logische toegang tot de persoonsgegevens wordt verleend middels een formeel proces en de verleende toegangsrechten worden geregistreerd, periodiek gecontroleerd en zo nodig herzien.
9. Medewerkers die onder verantwoordelijkheid van Verwerker de toegang verkrijgen tot gevoelige persoonsgegevens of een grote verzameling van minder gevoelige persoonsgegevens, overleggen voor aanvang van de werkzaamheden een Verklaring



Omtrent het Gedrag (VoG) aan Verwerker.

10. Tevens is tussen Verwerker en de hiervoor bedoelde medewerkers voor aanvang van de werkzaamheden een overeenkomst gesloten waarin bepaald is:
 - i. dat de verwerking van persoonsgegevens uitsluitend plaatsvindt in het kader van de door Verwerker geleverde diensten en voor zover dat noodzakelijk is voor het uitoefenen van de functie;
 - ii. dat strikte geheimhouding wordt betracht ten aanzien van de verwerkte persoonsgegevens;
 - iii. dat er kennis is genomen van de bij Verwerker geldende regels en voorschriften ten aanzien van de verwerking en beveiliging van persoonsgegevens;
 - iv. dat het niet volgen van de regels en voorschriften, in geval van opzet of grove nalatigheid kan leiden tot door Verwerker opgelegde sancties of schadevergoedingen.
11. Medewerkers krijgen door Verwerker geschikte training en regelmatige bijscholing aangeboden over het informatiebeveiligingsbeleid en de informatiebeveiligingsprocedures van de organisatie, voor zover relevant voor hun functie. Binnen de training en bijscholing wordt expliciet aandacht besteed aan de omgang met persoonsgegevens.
12. Iedere vorm van toegang, modificatie, duplicatie en verwijdering van de persoonsgegevens wordt door Verwerker op zodanige wijze vastgelegd dat de uitgevoerde transacties gedurende een periode van 6 maanden herleidbaar zijn tot de medewerkers die deze transactie hebben uitgevoerd, alsmede de tijdstippen waarop deze transactie zijn uitgevoerd.
13. Er zijn adequate procedures en maatregelen ingericht ter voorkomen van ongeautoriseerde aanpassing van de transactievastleggingen als bedoeld in de vorige maatregel en er is een proces ingericht ten behoeve van periodieke inspectie van de transactievastleggingen teneinde ongeautoriseerde of oneigenlijke toegang, modificatie, duplicatie of verwijdering van persoonsgegevens tijdig op te merken.
14. Er is een scheiding van verantwoordelijkheden en taken aangebracht tussen medewerkers die zorgdragen voor het beheersen, vastleggen en inspecteren van de toegang tot de persoonsgegevens en de medewerkers die ten behoeve van de uitoefening van hun functie daadwerkelijk toegang verkrijgen tot de persoonsgegevens.
15. Bijzondere of anderszins gevoelige persoonsgegevens alsmede grote verzamelingen persoonsgegevens worden in versleutelde vorm opgeslagen.
16. Persoonsgegevens worden uitsluitend in versleutelde vorm uitgewisseld bij verzending over niet-vertrouwde netwerken of bij transport op fysieke opslagmedia.
17. De sleutels voor het leesbaar maken van versleutelde persoonsgegevens worden beheerd in een formeel proces en de toegang tot de sleutels is beperkt tot medewerkers die hiertoe voor de uitoefening van hun functie de beschikking over dienen te hebben.
18. In toepassingssystemen waarop persoonsgegevens worden verwerkt, inclusief toepassingen die door gebruikers zelf zijn ontwikkeld, zijn beveiligingsmaatregelen ingebouwd ter controle dat de invoer, de interne verwerking en de uitvoer aan vooraf gestelde eisen voldoen.
19. Systemen waarop de verwerking van persoonsgegevens plaatsvindt zijn voorzien van anti-



malware voorzieningen en adequate beveiligingsmaatregelen ten behoeve van de beheersing van de toegang tot deze systemen.

20. Besturingssysteem, systeem- en applicatiesoftware die voor de verwerking van de persoonsgegevens onder verantwoordelijkheid van Verwerker aangewend wordt, wordt actief gemonitord op kwetsbaarheden in de beveiliging en is voorzien van de laatste software wijzigingen.
21. Software voor webapplicaties die voor de verwerking van de persoonsgegevens onder verantwoordelijkheid van Verwerker aangewend wordt, is ontworpen, ontwikkeld, getest en geconfigureerd op basis van gangbare normen voor veilige webapplicaties, waaronder OWASP en de NCSC richtlijn "ICT beveiligingsrichtlijnen voor Webapplicaties".

Aantonen passend niveau van beveiliging

Normenstelsel

De verwerker is verplicht volgens de volgende algemeen erkende normen voor informatiebeveiliging te werken:

- ☐ BIO,
- ☐ NEN/ISO 27001,

Of een aan bovenstaande normen gelijkwaardig normenstelsel, waarbij het bewijs voor gelijkwaardigheid aan de norm wordt geleverd door een onafhankelijke derde/auditor als bedoeld in het ISO-systeem.

Toereikendheid

Bij uitbesteding van beheer en exploitatie van informatiesystemen (dus ook SAAS-toepassingen) moet de toereikendheid van de informatiebeveiliging worden vastgesteld door de volgende op te leveren documenten.

1) en 2) zijn verplicht; 3) is verplicht bij webapplicaties en SAAS-toepassingen.

Verwerker is verplicht om jaarlijks aan Verwerkingsverantwoordelijke te overleggen:

- 1) Certificering van het verplichte normenstelsel en verklaring van toepasselijkheid (VVT)
- 2) Een assurance-rapport (TPM, bijvoorbeeld ISAE3402 of SOC type 2) van een onafhankelijke derde/auditor die ter zake aantoonbaar deskundig is;
- 3) Rapportages van pen/hacktesten bij webapplicaties en SAAS-toepassingen van een onafhankelijke derde/auditor die ter zake aantoonbaar deskundig is.



Bijlage 3: Melden van een datalek

Heeft u een datalek waarbij persoonsgegevens betrokken zijn waarvoor de VrAA Verwerkingsverantwoordelijke is? Dan meldt u het datalek conform eerder genoemde artikelen uit deze Verwerkersovereenkomst digitaal én telefonisch. Of het datalek voor VrAA al dan niet zichtbaar is heeft geen invloed op uw verplichting het datalek bij ons te melden.

U kunt bij VrAA melding doen van een (mogelijk) datalek door een e-mail met de vereiste informatie te sturen naar privacy@brandweeraa.nl. Daarnaast moet u telefonisch een melding doen van een (mogelijk) datalek. Dit doet u door te bellen naar 020-5556005.

Privacy contacten

Bij Verwerkingsverantwoordelijke: de Privacy Officer van de Veiligheidsregio Amsterdam-Amstelland.

Bij Verwerker:

Veiligheidsregio Amsterdam-Amstelland

Bezoekadres:
Ringdijk 98, 1097 AH Amsterdam

Postadres:
Postbus 92171, 1090 AD Amsterdam

Telefoon:
020 555 6550

Website:
veiligheidsregioaa.nl