

Bijlage F.

Concept Verwerkersovereenkomst VRZL

[Naam Dienst/Project/Applicatie/ Voorziening]

Registratienummer: <registratienummer uit DMS>

DE ONDERGETEKENDEN:

De publiekrechtelijke rechtspersoon Veiligheidsregio Zuid-Limburg, gevestigd op de Holstraat 35, 6269 AW, te Margraten en in deze rechtsgeldig vertegenwoordigd door: dhr. L.W.M. Houben MCDm (Directeur Veiligheidsregio Zuid-Limburg / Commandant Brandweer Zuid-Limburg), verder te noemen **'verwerkingsverantwoordelijke'**,

en

<Volledige naam en rechtsvorm bedrijf, afdeling>, gevestigd te <plaatsnaam>, <adres>, in deze rechtsgeldig vertegenwoordigd door de <de heer of mevrouw>, <persoonsnaam> , <functie>, verder te noemen de **'verwerker'**,

Hierna gezamenlijk te noemen: **'Partijen'** en individueel te noemen de **'Partij'**;

Nemen het volgende in aanmerking:

Partijen hebben op d.d. ...-...-.... een hoofdovereenkomst gesloten met kenmerk EA-VRZL-20230010 met betrekking tot de Openbare Europese Aanbesteding betreffende HRM systeem ten behoeve van Veiligheidsregio Zuid-Limburg;

In het kader van de uitvoering van de hoofdovereenkomst in de zin van artikel 4 sub 1 van de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG) worden persoonsgegevens verwerkt door verwerker, ten behoeve van verwerkingsverantwoordelijke;

Partijen wensen zorgvuldig en in overeenstemming met de AVG en andere toepasselijke wet- en regelgeving betreffende de verwerking van persoonsgegevens om te gaan met de persoonsgegevens die ter uitvoering van de Overeenkomst verwerkt (zullen) worden;

Partijen wensen in overeenstemming met artikel 28 derde lid van de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van persoonsgegevens hun rechten en plichten ten aanzien van de Verwerking van persoonsgegevens van Betrokkenen schriftelijk vast te leggen in deze overeenkomst.

Waar in deze verwerkersovereenkomst termen worden gebruikt die overeenstemmen met definities uit artikel 4 AVG, wordt aan deze termen de betekenis van de definities uit de AVG toegekend

EN ZIJN ALS VOLGT OVEREENGEKOMEN:

Artikel 1 Definities

AVG: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 (algemene verordening gegevensbescherming, AVG).

Toeziethouder: de Autoriteit Persoonsgegevens (AP) is het zelfstandig bestuursorgaan dat in Nederland bij wet als toezichthouder is aangesteld voor het toezicht op het verwerken van Persoonsgegevens.

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 Persoonsgegevens.

Betrokkene: de geïdentificeerde of identificeerbare natuurlijke persoon op wie de persoonsgegevens betrekking hebben, zoals bedoeld in artikel 4 onder 1) AVG, betrekking heeft.

Overeenkomst: de overeenkomst die tussen verwerkingsverantwoordelijke en verwerker is gesloten en op grond waarvan verwerker persoonsgegevens ten behoeve van de uitvoering van deze overeenkomst voor Verwerkingsverantwoordelijke verwerkt.

Persoonsgegevens: alle informatie over een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, zoals bedoeld in artikel 4 onder 1 AVG.

Statement of applicability: overzicht met ISO 27001 normen die op de organisatie van toepassing zijn verklaard en waarvoor maatregelen zijn geïmplementeerd t.b.v. de informatiebeveiliging.

Sub-verwerker: een andere verwerker, waaronder maar niet beperkt tot groepsmaatschappijen, zustermaatschappijen, dochtermaatschappijen en hulpleveranciers, die verwerker inschakelt om voor rekening van de Verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten. Degene die ten behoeve van de Verwerkingsverantwoordelijke persoonsgegevens verwerkt, in opdracht van de verwerker, is een sub-verwerker.

Paraaf Verwerkingsverantwoordelijke

Paraaf Verwerker

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 bedoeld in artikel 4 onder 2 AVG.

Verwerkersovereenkomst: de onderhavige overeenkomst inclusief bijlagen, zoals bedoeld in artikel 28 lid 3 AVG.

Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Artikel 2 Ingangsdatum en duur

- 2.1 Deze verwerkersovereenkomst treedt in werking vanaf datum van ondertekening door beide partijen en blijft van kracht tot de beëindiging of afloop van de hoofdovereenkomst.
- 2.2 Indien de hoofdovereenkomst eindigt, eindigt deze verwerkersovereenkomst.
- 2.3 Geen van beide partijen kan deze verwerkersovereenkomst tussentijds opzeggen.
- 2.4 Alle bepalingen van deze verwerkersovereenkomst die uitdrukkelijk of impliciet zijn bedoeld om van kracht te blijven na beëindiging of afloop van deze Verwerkersovereenkomst blijven volledig van kracht.

Artikel 3 Onderwerp van deze Verwerkersovereenkomst

- 3.1 De verwerker verwerkt de door of via verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens uitsluitend in opdracht van de verwerkingsverantwoordelijke in het kader van de uitvoering van de overeenkomst EA-VRZL-20230010.
- 3.2 De verwerkersovereenkomst vormt een aanvulling op de overeenkomst en vervangt eventuele eerder gemaakte afspraken tussen partijen ten aanzien van de verwerking van persoonsgegevens. Bij tegenstrijdigheid tussen de bepalingen uit de verwerkersovereenkomst en de overeenkomst, prevaleren de bepalingen uit de verwerkersovereenkomst.
- 3.3 De door de verwerker uit te voeren werkzaamheden waar deze verwerkersovereenkomst betrekking op heeft, worden nader, omschreven in bijlage 1. Verwerker zal, met inachtneming van artikel 28 AVG, de persoonsgegevens niet voor enig ander doel verwerken, behoudens afwijkende wettelijke verplichtingen.
- 3.4 De verwerker verbindt zich om in het kader van die werkzaamheden de door of via de Verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens zorgvuldig te verwerken.

Artikel 4 Verplichtingen Verwerker

- 4.1 De verwerker verwerkt gegevens ten behoeve van de Verwerkingsverantwoordelijke, in overeenstemming met diens schriftelijke instructies en in overeenstemming met de op haar rustende wettelijke verplichtingen op grond van de AVG of andere toepasselijke implementatiewetgeving van de AVG.
- 4.2 De verwerker heeft geen zeggenschap over de ter beschikking gestelde persoonsgegevens. Voor zover niet anders bepaald neemt verwerker geen beslissingen over de ontvangst en gebruik van de gegevens, de verstrekking aan derden en de duur van de opslag van gegevens. De zeggenschap over de persoonsgegevens verstrekt onder deze verwerkersovereenkomst komt nimmer bij de verwerker te berusten.
- 4.3 De verwerker zal bij de verwerking van persoonsgegevens in het kader van de in artikel 3 genoemde werkzaamheden, handelen in overeenstemming met de toepasselijke wet- en regelgeving betreffende de verwerking van persoonsgegevens. Indien sprake is van afwijkende wettelijke verplichtingen, dan wordt de contactpersoon, als bedoelt in artikel 12, vijfde lid hiervan, voorafgaand aan de verwerking, schriftelijk op de hoogte gebracht door de verwerker.
- 4.4 De verwerker zal te allen tijde op eerste verzoek van de contactpersoon, zoals bedoelt in artikel 12 vijfde lid, door de verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens met betrekking tot deze verwerkersovereenkomst ter hand stellen, tenzij deze persoonsgegevens conform nadere werkafspraken zijn verwijderd.
- 4.5 De verwerker stelt de verwerkingsverantwoordelijke te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG, meer in het bijzonder de rechten van betrokkenen, zoals, maar niet beperkt tot een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens en het uitvoeren van een gehonoreerd aangetekend verzet.

Artikel 5 Geheimhoudingsplicht

- 5.1 Personen in dienst van, dan wel werkzaam ten behoeve van de verwerker, evenals de verwerker zelf, zijn verplicht tot geheimhouding met betrekking tot de persoonsgegevens waarvan zij kennis kunnen nemen, behoudens voor zover een bij, of krachtens de wet gegeven voorschrift tot verstrekking verplicht. De medewerkers van de verwerker tekenen hiertoe een geheimhoudingsverklaring.
- 5.2 Indien de verwerker op grond van een wettelijke verplichting gegevens dient te verstrekken, zal de verwerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal de verwerker de verwerkingsverantwoordelijke onmiddellijk, voorafgaand aan de verstrekking, ter zake informeren. Tenzij wettelijke bepalingen dit verbieden.

Paraaf Verwerkingsverantwoordelijke

Paraaf Verwerker

Artikel 6 Meldplicht datalekken en beveiligingsincidenten

- 6.1 De verwerker zal de verwerkingsverantwoordelijke zo spoedig mogelijk - doch uiterlijk binnen 48 uur na de eerste ontdekking - informeren over alle (vermoedelijke) inbreuken op de beveiliging alsmede andere incidenten die op grond van wetgeving moeten worden gemeld aan de toezichthouder of betrokkene, onverminderd de verplichting de gevolgen van dergelijke inbreuken en incidenten zo snel mogelijk ongedaan te maken dan wel te beperken.
- 6.2 Verwerker zal voorts, op het eerste verzoek van de verwerkingsverantwoordelijke, alle inlichtingen verschaffen die de Verwerkingsverantwoordelijke noodzakelijk acht om het incident te kunnen beoordelen. Daarbij verschaft verwerker in ieder geval de informatie aan de verwerkingsverantwoordelijke zoals omschreven in bijlage 2.
- 6.3 De verwerker beschikt over een gedegen plan van aanpak betreffende de omgang met en afhandeling van inbreuken en zal de Verwerkingsverantwoordelijke, op diens verzoek, inzage verschaffen in het plan. Verwerker stelt de verwerkingsverantwoordelijke op de hoogte van materiele wijzigingen in het plan van aanpak.
- 6.4 De verwerker zal de meldingen aan de toezichthouder(s) overlaten aan de verwerkingsverantwoordelijke.
- 6.5 De verwerker zal alle noodzakelijke medewerking verlenen aan het zo nodig, op de kortst mogelijke termijn, verschaffen van aanvullende informatie aan de toezichthouder(s) en/of betrokkene(n). Daarbij verschaft verwerker in ieder geval de informatie, zoals beschreven in bijlage 2, aan de verwerkingsverantwoordelijke.
- 6.6 De verwerker houdt een gedetailleerd logboek bij van alle vermoedens van inbreuken op de beveiliging, evenals de maatregelen die in vervolg op dergelijke inbreuken zijn genomen waarin minimaal de informatie zoals bedoeld in bijlage 2 is opgenomen, en geeft daar op eerste verzoek van de verwerkingsverantwoordelijke inzage in.

Artikel 7 Beveiligingsmaatregelen en controle

- 7.1 De verwerker neemt alle passende technische en organisatorische maatregelen om de persoonsgegevens welke worden verwerkt ten dienste van de Verwerkingsverantwoordelijke te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van onrechtmatige verwerking. De wijze van beveiliging wordt nader omschreven in bijlage 3.
- 7.2 De Verwerkingsverantwoordelijke is te allen tijde gerechtigd de verwerking van persoonsgegevens te (doen) controleren. De verwerker is verplicht de verwerkingsverantwoordelijke, de Autoriteit persoonsgegevens, of, de onder geheimhouding, controlerende instantie in opdracht van verwerkingsverantwoordelijke toe te laten en verplicht medewerking te verlenen zodat de controle daadwerkelijk uitgevoerd kan worden.
- 7.3 De verwerkingsverantwoordelijke zal de controle slechts (laten) uitvoeren na een voorafgaande schriftelijke melding aan de verwerker.

Paraaf Verwerkingsverantwoordelijke

Paraaf Verwerker

- 7.4 De verwerker verbindt zich om binnen een door de verwerkingsverantwoordelijke te bepalen redelijke termijn de verwerkingsverantwoordelijke, of de door de verwerkingsverantwoordelijke ingeschakelde derde, te voorzien van de verlangde informatie. Hierdoor kan de Verwerkingsverantwoordelijke, of de door de Verwerkingsverantwoordelijke ingeschakelde derde, zich een oordeel vormen over de naleving door de verwerker van deze verwerkersovereenkomst. De verwerkingsverantwoordelijke, of de door de verwerkingsverantwoordelijke ingeschakelde derde, is gehouden alle informatie betreffende deze controles vertrouwelijk te behandelen.
- 7.5 Verwerker staat er voor in, de door de Verwerkingsverantwoordelijke of ingeschakelde derde, aangegeven aanbevelingen ter verbetering binnen de daartoe door de verwerkingsverantwoordelijke te bepalen redelijke termijn uit te voeren.
- 7.6 De verwerker rapporteert jaarlijks over de opzet en werking van het stelsel van maatregelen en procedures, gericht op naleving van deze verwerkersovereenkomst.
- 7.7 De redelijke kosten van de controle worden gedragen door de partij die de kosten maakt tenzij uit de controle blijkt dat verwerker nalatig is in de opvolging van de uitspraken uit deze verwerkersovereenkomst. In dat geval worden de kosten van controle gedragen door de verwerker.

Artikel 8 Inschakeling derden

- 8.1 De verwerker is slechts gerechtigd de uitvoering van de werkzaamheden geheel of ten dele uit te besteden aan derden na voorafgaande, duidelijk gespecificeerde, schriftelijke toestemming van de verwerkingsverantwoordelijke.
- 8.2 De Verwerkingsverantwoordelijke kan aan de schriftelijke toestemming voorwaarden verbinden, op het gebied van geheimhouding en ter naleving van de verplichtingen uit deze verwerkersovereenkomst.
- 8.3 De verwerkingsverantwoordelijke geeft de verwerker toestemming om, in het kader van de bovenliggende overeenkomst en de in de bijlage 4 bedoelde gegevensverwerking derden (sub-verwerkers) in te schakelen. Deze subverwerkers dienen minimaal te voldoen aan dezelfde eisen in het kader van de AVG (Bijvoorbeeld ISO 27001 of BIR of gelijkwaardig). Verwerker zal verwerkingsverantwoordelijke, of dienst branchevertegenwoordiging, informeren over welke sub-verwerker zij inschakelt.
- 8.4 De verwerker blijft in deze gevallen te allen tijde aanspreekpunt en verantwoordelijk voor de naleving van de bepalingen uit deze verwerkersovereenkomst. De verwerker garandeert dat deze derden schriftelijk minimaal dezelfde plichten op zich nemen als tussen de verwerkingsverantwoordelijke en de verwerker zijn overeengekomen en zal de verwerkingsverantwoordelijke, op diens verzoek, inzage verschaffen in de overeenkomsten met deze derden waarin deze plichten zijn opgenomen.
- 8.5 De Verwerker zal geen Persoonsgegevens verwerken in of doorgeven aan een land, gebied of organisatie buiten de Europese Unie zonder voorafgaande

Paraaf Verwerkingsverantwoordelijke

Paraaf Verwerker

schriftelijke toestemming van de verwerkingsverantwoordelijke (en de verwerker zorgt ervoor dat de door hem ingeschakelde derden aan hetzelfde voldoen).

- 8.6 De verwerker houdt een actueel register bij van de door hem ingeschakelde derden en onderaannemers waarin de identiteit, vestigingsplaats en een beschrijving van de werkzaamheden van de derden of onderaannemers zijn opgenomen, alsmede eventuele door de verwerkingsverantwoordelijke gestelde aanvullende voorwaarden. Verwerker zal de contactpersoon van de verwerkingsverantwoordelijke inzage verlenen in dit register of dit register zal, zoals nader omschreven in bijlage 4, aan deze verwerkersovereenkomst worden toegevoegd en zal door de verwerker actueel worden gehouden.

Artikel 9 Wijziging en beëindiging verwerkersovereenkomst

- 9.1 Wijziging van deze verwerkersovereenkomst kan slechts schriftelijk plaatsvinden middels een door beide partijen geaccordeerd voorstel.
- 9.2 Zodra de samenwerking is beëindigd, zal de verwerker naar keuze van de verwerkingsverantwoordelijke
- (i) alle of een door verwerkingsverantwoordelijke bepaald gedeelte van haar in het kader van deze verwerkersovereenkomst ter beschikking gestelde persoonsgegevens aan de verwerkingsverantwoordelijke ter beschikking stellen.
- (ii) de persoonsgegevens die hij van de verwerkingsverantwoordelijke heeft ontvangen op alle locaties vernietigen, in welke vorm dan ook en toont dit aan, tenzij partijen iets anders overeenkomen.
- De verwerkingsverantwoordelijke kan zo nodig nadere eisen stellen aan de wijze van beschikbaarstelling, waaronder eisen aan het bestandsformaat, dan wel vernietiging. Deze werkzaamheden moeten, binnen nader overeen te komen redelijke termijn, uitgevoerd worden en hiervan wordt een verslag gemaakt.
- 9.3 De verwerker zal te allen tijde de in het vorig lid beschreven recht op (dataportabiliteit) overdraagbaarheid van gegevens conform artikel 20 AVG waarborgen, zodanig dat er geen sprake is van verlies van functionaliteit of (delen van) de gegevens.
- 9.4 Verwerkingsverantwoordelijke en verwerker treden met elkaar in overleg over wijzigingen in deze verwerkersovereenkomst als een wijziging in regelgeving, een wijziging in de uitleg van regelgeving of wijziging in de verwerking van persoonsgegevens daartoe aanleiding geven.
- 9.5 Indien een partij tekortschiet in de nakoming van een overeengekomen verplichting, kan de andere partij haar in gebreke stellen waarbij de nalatige partij alsnog een redelijke termijn voor de nakoming wordt gegund. Blijft nakoming ook dan uit dan is de nalatige partij in verzuim. Ingebrekestelling is niet nodig wanneer voor de nakoming een fatale termijn geldt, nakoming blijvend onmogelijk is of indien uit een mededeling dan wel de houding van de andere partij moet worden afgeleid dat deze in de nakoming van haar verplichting zal tekortschieten.

- 9.6 Verwerkingsverantwoordelijke is gerechtigd deze verwerkersovereenkomst en de overeenkomst per direct te ontbinden indien verwerker te kennen geeft niet (langer) te kunnen voldoen aan de betrouwbaarheidseisen of als de verwerkingsverantwoordelijke gerede twijfel heeft of de verwerker aan de betrouwbaarheidseisen, die op grond van ontwikkelingen in de wet en/of de rechtspraak aan de verwerking van de persoonsgegevens worden gesteld

Artikel 10 Aansprakelijkheid

- 10.1 Indien de verwerker tekortschiet in de nakoming van de verplichtingen uit deze verwerkersovereenkomst kan verwerkingsverantwoordelijke haar in gebreke stellen. verwerker is echter onmiddellijk in gebreke als de nakoming van desbetreffende verplichting anders dan door overmacht binnen de overeengekomen termijn, reeds blijvend onmogelijk is. Ingebrekestelling geschiedt schriftelijk, waarbij aan de verwerker een redelijke termijn wordt gegund om alsnog haar verplichtingen na te komen. Deze termijn is een fatale termijn. Indien nakoming binnen deze termijn uitblijft, is verwerker in verzuim.
- 10.2 Verwerker is aansprakelijk op grond van het bepaalde in artikel 82 AVG, voor schade of nadeel voortvloeiende uit het niet nakomen van deze verwerkersovereenkomst, daaronder begrepen wanneer bij de verwerking niet wordt voldaan aan de specifiek tot verwerkingsgerichte verplichtingen van de AVG, of buiten de rechtmatige instructies van verwerkingsverantwoordelijke is gehandeld of bij strijdigheid ingeval van het niet nakomen van de AVG en andere toepasselijke wet- en regelgeving.
- 10.3 Verwerker vrijwaart verwerkingsverantwoordelijke voor schade of nadeel voor zover ontstaan door werkzaamheid van de verwerker.
- 10.4 Indien verwerker de in artikel 6 lid 1 van deze verwerkersovereenkomst neergelegde verplichting niet of niet-tijdig nakomt en de Toezichthouder de verwerkingsverantwoordelijke dientengevolge een bestuurlijke boete oplegt, is verwerker aansprakelijk en zal verwerkingsverantwoordelijke een contractuele boete ter hoogte van hetzelfde bedrag opleggen aan verwerker. Deze boete is niet vatbaar voor verrekening en opschorting en laat de rechten van verwerkingsverantwoordelijken op nakoming en schadevergoeding onverlet.

Artikel 11 Toepasselijk recht

- 11.1 De verwerkersovereenkomst en de uitvoering daarvan worden beheerst door Nederlands recht.
- 11.2 Alle geschillen, die tussen partijen ontstaan in verband met de verwerkersovereenkomst, zullen worden voorgelegd aan de bevoegde rechter in de plaats waar verwerkingsverantwoordelijke is gevestigd.

Paraaf Verwerkingsverantwoordelijke

Paraaf Verwerker

Artikel 12 Overige bepalingen/ Slotbepalingen

- 12.1 Deze verwerkersovereenkomst kan worden aangehaald als <'Titel'>.
- 12.2 Afwijkingen van deze verwerkersovereenkomst zijn slechts bindend voor zover zij uitdrukkelijk tussen Partijen schriftelijk zijn overeengekomen.
- 12.3 Algemene leveringsvoorwaarden dan wel andere algemene of bijzondere voorwaarden van verwerker die afwijken van het bepaalde in deze verwerkersovereenkomst zijn niet van toepassing en worden door verwerkingsverantwoordelijke uitdrukkelijk van de hand gewezen.
- 12.4 Deze verwerkersovereenkomst vormt een aanvulling op de overeenkomst. Bij strijdigheid tussen bepalingen uit deze verwerkersovereenkomst prevaleren de bepalingen uit de verwerkersovereenkomst.
- 12.5 De FG (Functionaris Gegevensverwerking) van Veiligheidsregio Limburg Zuid treedt namens de verwerkingsverantwoordelijke op als contactpersoon.

Aldus in tweevoud opgemaakt en ondertekend door de partijen:

Verwerkingsverantwoordelijke:

Veiligheidsregio Zuid-Limburg

Plaats: Sittard

Datum: ..-..-....

Verwerker:

.....

Plaats:

Datum: ..-..-....

Dhr. L.W.M. Houben MCDm

.....

Directeur Veiligheidsregio / Commandant Brandweer

.....

Bijlage 1 Instructie verwerking van Persoonsgegevens

[Nader in te vullen. In deze bijlage moet in ieder geval het volgende nader worden gespecificeerd:

- de activiteiten in het kader waarvan Persoonsgegevens worden Verwerkt, eventueel onder verwijzing naar de Overeenkomst;
- welke Verwerkingen plaatsvinden, betrek daarbij in voorkomend geval onder andere het transporteren van gegevens en het maken van een back-up, door Verwerker;
- naam van de Verwerking(en);
- het doel of de doeleinden van de Verwerking(en);
- om welke Persoonsgegevens van welke categorieën Betrokkenen het gaat;
- de duur van de Verwerking, voor zover die afwijkt van de duur van de Overeenkomst

Paraaf Verwerkingsverantwoordelijke

Paraaf Verwerker

Bijlage 2 Lijst aan te leveren info datalek/incident (zie artikel 6 lid 5)

De verwerker zal, conform artikel 33 AVG alle inlichtingen verschaffen die de verwerkingsverantwoordelijke noodzakelijk acht om het incident te kunnen beoordelen. Daarbij verschaft verwerker in ieder geval de volgende informatie aan de verwerkingsverantwoordelijke:

1. de (vermeende) oorzaak van de inbreuk;
2. het (vooralsnog bekende en/of te verwachten) gevolg;
3. de (voorgestelde) oplossing;
4. contactgegevens voor de opvolging van de melding;
5. aantal personen waarvan gegevens betrokken zijn bij de inbreuk (indien geen exact aantal bekend is: het minimale en maximale aantal personen waarvan gegevens betrokken zijn bij de inbreuk);
6. een omschrijving van de groep personen van wie gegevens betrokken zijn bij de inbreuk;
7. het soort of de soorten persoonsgegevens die betrokken zijn bij de inbreuk;
8. de datum waarop de inbreuk heeft plaatsgevonden (indien geen exacte datum bekend is: de periode waarbinnen de inbreuk heeft plaatsgevonden);
9. de datum en het tijdstip waarop de inbreuk bekend is geworden bij verwerker of bij een door hem ingeschakelde derde of onderaannemer;
10. of de gegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk zijn gemaakt voor onbevoegden;
11. de reeds ondernomen maatregelen om de inbreuk te beëindigen en om de gevolgen van de inbreuk te beperken.

Paraaf Verwerkingsverantwoordelijke

Paraaf Verwerker

Bijlage 3 Organisatorische en technische maatregelen voor de beveiliging

Verwerker heeft een (informatie)beveiligingsbeleid opgesteld en de hierin beschreven maatregelen aantoonbaar geïmplementeerd. Dit beleid wordt met regelmaat getoetst en geactualiseerd. De beveiligingsmaatregelen zijn passend voor en in overeenstemming met de waarde van de te verwerken gegevens.

Wanneer verwerker gebruik maakt van subverwerkers, dienen deze expliciet te zijn beschreven en bekend te zijn bij verwerkingsverantwoordelijke. De subverwerker houdt zich aan minimaal dezelfde beveiligingseisen en – maatregelen als verwerker.

Organisatie van informatiebeveiliging

Verantwoordelijkheden ten aanzien van het beschermen van persoonsgegevens zijn binnen de organisatie van verwerker expliciet benoemd en belegd.

Personele maatregelen

Verwerker heeft aantoonbaar bevoegd en bekwaam personeel. Zowel bevoegd en bekwaam voor het verwerken van de gegevens als voor het beveiligen en beschermen van de gegevens.

De personeelsleden zijn via een schriftelijke overeenkomst verplicht tot geheimhouding van alle informatie van verwerkingsverantwoordelijke.

Toegang tot Persoonsgegevens

Toegang tot persoonsgegevens is beperkt op basis van het need-to-know principe. Alleen wanneer toegang tot persoonsgegevens daadwerkelijk benodigd is voor het uitvoeren van de werkzaamheden wordt deze toegang ook ingeregeld. Zodra bevoegdheden van personen veranderen, wordt de toegang tot gegevens hierop aangepast.

Verwerking op mobiele apparatuur

Wanneer persoonsgegevens worden verwerkt op mobiele apparatuur, waaronder tablets, laptops en/of smartphones, dan dienen deze apparaten versleuteld (encrypted) te zijn conform marktstandaarden.

Fysieke beveiliging

Verwerker zorgt ervoor dat persoonsgegevens worden verwerkt in een fysiek beveiligde omgeving, met passende bescherming tegen dreigingen van buitenaf.

IT-technische maatregelen

Verwerker neemt passende maatregelen om de IT-omgeving te beveiligen. Informatiesystemen, componenten en middelen zijn actueel en worden door de fabrikant officieel ondersteund.

Paraaf Verwerkingsverantwoordelijke

Paraaf Verwerker

Alle software wordt op basis van een gestructureerd proces voorzien van de laatste patches. Waar technisch mogelijk wordt gebruik gemaakt van antivirussoftware.

Netwerken en informatiesystemen worden passend afgeschermd op basis van fysieke of logische scheiding, waarbij wordt gewaarborgd dat informatie van verwerkingsverantwoordelijke niet vermengd kan worden met dat van andere klanten van verwerker.

Wanneer informatie over openbare netwerken of anderszins publiek beschikbaar kan komen, worden cryptografische maatregelen genomen om de informatie te beschermen tegen onbevoegde inzage.

Periodiek worden vulnerability scans en penetratietests uitgevoerd voor het toetsen van de beveiliging.

Toegang op afstand

Wanneer medewerkers van verwerker toegang op afstand (bijvoorbeeld telewerken via internet) kunnen krijgen tot persoonsgegevens, is deze toegang afgeschermd met een versleutelde verbinding. Toegang op afstand kan alleen worden verkregen door middel van het toepassen van 2 factor authenticatie.

Beheer van incidenten

Verwerker verplicht zijn medewerkers incidenten met betrekking tot informatiebeveiliging en privacy zo snel mogelijk te melden en deze op basis van de ernst op te volgen. Enkele voorbeelden van incidenten zijn:

- Uitval van dienstverlening, apparatuur of voorzieningen; Systeemstoringen of –overbelasting;
- Menselijke fouten;
- Niet-naleven van beleid en/of richtlijnen;
- Inbreuk op fysieke beveiligingsmaatregelen; Ongecontroleerde systeemwijzigingen;
- Storingen aan software of hardware; Virusuitbraak;
- Toegangsovertredingen (digitaal of fysiek).

Alle medewerkers, tijdelijke medewerkers, onderaannemers en derde partijen die op enigerlei wijze gebruik maken van informatie of informatiesystemen van verwerker zijn verplicht om (mogelijke) lekken en inbreuken in de informatiebeveiliging te melden als incident. Hiertoe wordt aan deze betrokkenen het incidentmeldingsproces van verwerker kenbaar gemaakt.

Verwerker monitort toegang tot persoonsgegevens en het mogelijk lekken hiervan.

Paraaf Verwerkingsverantwoordelijke

Paraaf Verwerker

Continuïteit van de dienstverlening

Verwerker neemt binnen de dienstverlening passende technische en organisatorische maatregelen om continuïteit te waarborgen. Wanneer de overeenkomst tussen verwerkingsverantwoordelijke en verwerker eindigt, verplicht verwerker zich te zorgen dat de dienstverlening van Verwerkingsverantwoordelijke gewaarborgd blijft in de transitie naar de nieuwe leverancier van verwerkingsverantwoordelijke.

Overige maatregelen

De maatregelen beschreven in deze bijlage pretenderen niet concreet of volledig te zijn. Verwerkingsverantwoordelijke verwacht dat verwerker zich actief opstelt bij het beschermen van persoonsgegevens en het nemen van maatregelen om deze te beschermen. In wederzijds overleg kunnen verbeteringen ten aanzien van de verwerkersovereenkomst en de beschreven maatregelen worden besproken.

Paraaf Verwerkingsverantwoordelijke

Paraaf Verwerker

Bijlage 4 Lijst Sub-verwerkers

Omschrijving werkzaamheden derden ter uitwerking van art. 8.6 –