BIJLAGE PRIVACY EN VERWERKING PERSOONSGEGEVENS
X-GUARD ALS OPDRACHTNEMER

1 ALGEMEEN

1.1 Deze Bijlage Privacy en Verwerking Persoonsgegevens (de "**Bijlage**") is een bijlage bij de Overeenkomst. Definities in de Bijlage hebben dezelfde betekenis als in de Overeenkomst, tenzij uitdrukkelijk anders is aangegeven in artikel 18 (Definities). In geval van een conflict of tegenstrijdigheid tussen de Bijlage en de Overeenkomst prevaleren de bepalingen van de Bijlage.

1.2 Deze Bijlage is overeengekomen tussen X-Guard B.V. (hierna: X-Guard) en Opdrachtgever (en haar eventuele groepsmaatschappijen indien Opdrachtgever gerechtigd is namens haar groepsmaatschappijen deze Bijlage te handhaven).

2 INSTRUCTIES

2.1 X-Guard treedt op als Verwerker en mag de Persoonsgegevens die Opdrachtgever aan X-Guard verstrekt uitsluitend Verwerken op basis van schriftelijke instructies van Opdrachtgever en voor de doeleinden zoals vastgesteld door Opdrachtgever. X-Guard informeert Opdrachtgever onmiddellijk als naar mening van X-Guard een instructie inbreuk oplevert op de Toepasselijke Wetgeving.

2.2 Opdrachtgever instrueert X-Guard hierbij om de Persoonsgegevens te Verwerken overeenkomstig **Appendix I** (*Specificatie van Verwerkingen*).

2.3 X-Guard mag geen Persoonsgegevens Verwerken voor haar eigen doeleinden zonder voorafgaande schriftelijke toestemming van Opdrachtgever. Als X-Guard Persoonsgegevens Verwerkt voor haar (i) eigen doeleinden of (ii) doeleinden die niet zijn vastgesteld door Opdrachtgever, dan is X-Guard de Verwerkingsverantwoordelijke voor die verwerken en is zij onderworpen aan Toepasselijke Wetgeving.

3 TOEPASSELIJK RECHT

3.1 Bij de verwerking van Persoonsgegevens voldoet X-Guard aan de Toepasselijke Wetgeving.

3.2 X-Guard verleent onverwijld en adequaat medewerking aan verzoeken van Opdrachtgever om ervoor te zorgen dat de Verwerking geschiedt in overeenstemming met Toepasselijke Wetgeving.

4 BEVEILIGING

X-Guard legt passende technische, fysieke en organisatorische maatregelen ten uitvoer om de Persoonsgegevens te beveiligen tegen onbedoeld of onrechtmatig tenietgaan of onbedoeld verlies, onbedoelde wijziging, onbevoegde Openbaarmaking of onbevoegde terbeschikkingstelling en tegen alle andere vormen van onrechtmatige Verwerking inclusief, maar niet beperkt tot, onnodige verzameling en verdere Verwerking. Deze maatregelen garanderen een passend beveiligingsniveau, rekening houdend met de stand van de techniek en kosten van de tenuitvoerlegging van de maatregelen alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst

uiteenlopende risico's voor de rechten en vrijheden van personen, gelet op de risico's die de Verwerking en de aard van de te beschermen Persoonsgegevens met zich brengen. De maatregelen die X-Guard moet treffen zijn nader gespecificeerd in **Appendix II** (*Beveiligingsmaatregelen*) bij deze Bijlage, welke Appendix X-Guard/Verwerker aanpast wanneer dit nodig is om te voldoen aan de gebruikelijke marktstandaarden.

5 NIET-OPENBAARMAKING EN GEHEIMHOUDING

5.1 X-Guard houdt de Persoonsgegevens geheim en mag deze niet toegankelijk maken voor enige Medewerker (ook zijnde Medewerker Opdrachtgever) of Derden zonder de vooraf verkregen schriftelijke toestemming van de Privacy Officer van de Opdrachtgever, behalve (i) wanneer Openbaarmaking conform Artikel 5.3-6.2 van de Bijlage nodig is voor het uitvoeren van Verwerkingen, of (ii) conform Artikel 9.1(b) van de Bijlage, wanneer Persoonsgegevens moeten worden Geopenbaard aan een bevoegde publieke toezichthouder om te voldoen aan een wettelijke verplichting of zoals vereist voor auditdoeleinden.

5.2 X-Guard administreert elke Openbaarmaking minimaal zes maanden, behalve wanneer de AVG een andere termijn voorschrijft. De registratie omvat, maar is niet beperkt tot de:

(a) Naam en adresgegevens van de Derde aan wie de Persoonsgegevens zijn Geopenbaard;

(b) De soort Persoonsgegevens die zijn Geopenbaard;

(c) Data en het tijdstip waarop de Persoonsgegevens zijn Geopenbaard; en

(d) Doeleinden van de Openbaarmaking.

5.3 X-Guard mag Medewerkers alleen toegang verlenen tot de Persoonsgegevens voor zover dit nodig is om de Verwerkingen uit te voeren. X-Guard waarborgt dat de tot het Verwerken van de Persoonsgegevens gemachtigde Medewerkers zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden en draagt er zorg voor dat elke Medewerker die Persoonsgegevens verwerkt de geheimhouding en beveiliging van de Persoonsgegevens respecteert en handhaaft.

6 SUB-VERWERKERS

6.1 X-Guard mag Sub-Verwerkers geen Persoonsgegevens laten Verwerken zonder vooraf verkregen schriftelijke toestemming van Opdrachtgever. Elke toestemming van Opdrachtgever om Sub-Verwerkers in te zetten bij de Verwerking van Persoonsgegevens is onder de voorwaarde dat X-Guard volledig aansprakelijk blijft jegens Opdrachtgever voor de uitvoering van het contract door Sub-Verwerkers en al het overige handelen of nalaten van Sub-Verwerkers in verband met de Verwerking.

6.2 X-Guard draagt er zorg voor dat Sub-Verwerkers contractueel gebonden zijn aan dezelfde verplichtingen in verband met de Verwerking als die waar X-Guard op grond van de Overeenkomst, inclusief de Bijlage, aan is gebonden.

7 AUDIT EN COMPLIANCE

7.1 X-Guard stelt de systemen die worden gebruikt voor de Verwerking van Persoonsgegevens beschikbaar voor een audit door Opdrachtgever of een door Opdrachtgever aangewezen gekwalificeerde onafhankelijke auditor en verleent alle medewerking die Opdrachtgever redelijkerwijs nodig heeft voor het uitvoeren van een dergelijke audit. Als de audit uitwijst dat X-Guard is tekortgeschoten in de nakoming van enige verplichting op grond van de Bijlage, herstelt X-Guard de tekortkoming(en) onmiddellijk. In alle gevallen draagt Opdrachtgever de kosten voor het uitvoeren van de audit.

7.2 Opdrachtgever:

(a) stelt X-Guard tijdig op de hoogte van haar voornemen audit uit te voeren;

(b) zorgt ervoor dat haar vertegenwoordigers die de audit uitvoeren voldoen aan de redelijke regels van X-Guard omtrent vertrouwelijkheid, gezondheid en veiligheid die X-Guard meedeelt aan Opdrachtgever; en

(c) zorgt ervoor dat haar vertegenwoordigers die de audit uitvoeren zich in redelijkheid inspannen om onderbrekingen van de bedrijfsprocessen van X-Guard die het gevolg zijn van het uitoefenen de audit tot een minimum te beperken.

8 INSPECTIE OF ONDERZOEK DOOR PUBLIEKE TOEZICHTHOUDER

8.1 X-Guard verleent aan een bevoegde publieke toezichthouder toegang tot de voor Verwerking relevante systemen, faciliteiten en ondersteunende documentatie, indien dit nodig is om te voldoen aan een wettelijke verplichting. In geval van een inspectie of onderzoek verlenen beide partijen de nodige assistentie aan elkaar. Als een bevoegde publieke toezichthouder oordeelt dat het Verwerken onder de Overeenkomst onrechtmatig is, treffen beide partijen onmiddellijk maatregelen om naleving van de AVG en Toepasselijke Verwerkerswetgeving te bewerkstelligen.

9 MELDINGEN VAN OPENBAARMAKINGEN EN DATALEKKEN

9.1 X-Guard brengt Opdrachtgever onverwijld, en in elk geval binnen vierentwintig (24) uur, op de hoogte als:

(a) zij in verband met de Verwerkingen een vordering, gebod om in de rechtbank te verschijnen als getuige of deskundige of verzoek van een bevoegde publieke toezichthouder tot het uitvoeren van een inspectie of onderzoek heeft ontvangen, behalve wanneer het X-Guard wettelijk verboden is om Opdrachtgever daarvan op de hoogte te stellen;

(b) zij voornemens is om Persoonsgegevens te Openbaren aan een bevoegde publieke toezichthouder; of

(c) zij ontdekt of redelijkerwijs vermoedt dat er een Datalek heeft plaatsgevonden.

9.2 In het geval van een Datalek treft X-Guard onverwijld herstelmaatregelen. Verder voorziet X-Guard Opdrachtgever van alle relevante informatie die Opdrachtgever met betrekking tot het Datalek verzoekt. In dit kader verstrekt X-Guard aan Opdrachtgever in ieder geval de volgende informatie:

(a) de aard van de inbreuk;

(b) de aanbevolen maatregelen om negatieve gevolgen van de inbreuk te vermijden of te beperken;

(c) een beschrijving van de geconstateerde en vermoedelijke gevolgen van de inbreuk voor de verwerking van Persoonsgegevens en de maatregelen die X-Guard heeft getroffen en/of voorstelt te treffen om deze gevolgen te verhelpen.

X-Guard verleent volledige medewerking aan Opdrachtgever bij het tot stand brengen en het uitvoeren van een *response plan* om het Datalek te adresseren. X-Guard werkt op verzoek van Opdrachtgever mee aan het adequaat informeren van de betrokken Individuen. De betrokken Individuen hebben recht op inzage in de Persoonsgegevens die onderwerp zijn of zijn geweest van het Datalek.

10 MEDEWERKING BIJ KLACHTEN, VERZOEKEN EN VRAGEN

10.1 X-Guard behandelt vragen en verzoeken van Opdrachtgever over de Verwerking onder de Overeenkomst onverwijld en adequaat.

10.2 X-Guard informeert Opdrachtgever onverwijld over klachten, verzoeken of vragen van Individuen, inclusief maar niet beperkt tot verzoeken tot het wijzigen, verwijderen, beperken of blokkeren van Persoonsgegevens of het verkrijgen van een kopie daarvan. Op verzoek van Opdrachtgever zal X-Guard bijstand verlenen aan Opdrachtgever bij het behandelen van klachten, verzoeken of vragen. De kosten die hiermee gemoeid zijn komen voor rekening van Opdrachtgever. X-Guard mag zich niet rechtstreeks tot het Individu wenden behalve wanneer Opdrachtgever dit specifiek heeft geïnstrueerd.

11 REGISTER VAN VERWERKINGSACTIVITEITEN

X-Guard houdt een register bij van verwerkingsactiviteiten die namens Opdrachtgever worden uitgevoerd in overeenstemming met artikel 30 (2) van de AVG. Op verzoek van Opdrachtgever zal X-Guard onmiddellijk een kopie van de relevante verwerkingsactiviteiten aan Opdrachtgever verstrekken.

12 MEDEWERKING

12.1 Op verzoek van Opdrachtgever, zal X-Guard bijstand verlenen aan Opdrachtgever bij het doen nakomen van de verplichtingen van de Opdrachtgever uit hoofde van de artikelen 32 tot en met 36 AVG in verband met de uitvoering van de Overeenkomst en deze Bijlage.

12.2 X-Guard zal ervoor zorgen dat de relevante Sub-verwerkers, op kosten en uitgaven van X-Guard, volledig samenwerken met de Opdrachtgever bij het uitvoeren van gegevensbeschermingseffectbeoordeling in verband met de uitvoering van deze Overeenkomst.

13 MELDEN VAN NIET-NAKOMING EN HET RECHT OM TE SCHORSEN OF OP TE ZEGGEN

13.1 X-Guard meldt Opdrachtgever onverwijld als X-Guard:

(a) om welke reden dan ook niet kan voldoen aan haar verplichtingen uit de Bijlage; of

(b) zich bewust wordt van omstandigheden of veranderingen in de Toepasselijke Verwerkerswetgeving die het nakomen van haar verplichtingen onder de Bijlage substantieel bemoeilijken.

13.2 Als X-Guard niet kan voldoen aan zijn verplichtingen onder de Bijlage is Opdrachtgever, zonder afbreuk te doen aan de Overeenkomst, bevoegd om de Verwerking tijdelijk geheel of gedeeltelijk te schorsen tot de niet-nakoming is hersteld. Voor zover herstel niet mogelijk is, is Opdrachtgever bevoegd om het desbetreffende deel van de Verwerking door X-Guard met onmiddellijke ingang op te zeggen. Opdrachtgever is ook bevoegd om de Overeenkomst met onmiddellijke ingang op te zeggen als de schorsing van de Verwerking op grond van deze bepaling door Opdrachtgever een periode van zes (6) maanden overschrijdt.

14 RETOURNEREN EN VERNIETIGEN VAN PERSOONSGEGEVENS

Bij de beëindiging van de Overeenkomst retourneert X-Guard de Persoonsgegevens en alle kopieën daarvan aan Opdrachtgever en/of vernietigt alle Persoonsgegevens volgens instructie van Opdrachtgever, behalve wanneer de Overeenkomst of Toepasselijke Verwerkerswetgeving anders aangeeft. In dat geval Verwerkt X-Guard de Persoonsgegevens niet langer, behalve voor zover vereist op grond van de Overeenkomst of Toepasselijke Verwerkerswetgeving. Opdrachtgever mag X-Guard verzoeken om spoedig, en in elk geval binnen vierentwintig (24) uur, en schriftelijk te bevestigen en te garanderen dat X-Guard alle Persoonsgegevens en kopieën daarvan heeft geretourneerd en/of vernietigd. X-Guard staat op verzoek van Opdrachtgever een audit van de Verwerkingssystemen toe om Opdrachtgever te laten verifiëren dat X-Guard aan alle verplichtingen onder Artikel 14 heeft voldaan.

15 VRIJWARING

15.1 X-Guard vrijwaart Opdrachtgever en zal Opdrachtgever gevrijwaard houden van alle vorderingen, procedures of acties tegen Opdrachtgever ingesteld door een bevoegde publieke toezichthouder of Individu en die verband houden met het Verwerken door X-Guard en/of Sub-Verwerker(s). X-Guard vrijwaart Opdrachtgever en zal Opdrachtgever ook gevrijwaard houden van alle vorderingen, procedures of acties tegen Opdrachtgever die voortkomen uit een schending van de verplichting tot het beschermen van Persoonsgegevens door Verwerker en/of Sub-Verwerker(s) op grond van de Overeenkomst.

15.2 X-guard vrijwaart Opdrachtgever en zal Opdrachtgever gevrijwaard houden van alle kosten die verband houden met een Datalek, wanneer het Datalek is veroorzaakt door of is toe te rekenen aan een tekortkoming door X-Guard in de nakoming van de Overeenkomst, daarin begrepen de verplichtingen van X-Guard tot het beschermen van Persoonsgegevens op grond van de Overeenkomst en de Bijlage.

16 DOORGIFTE VAN PERSOONSGEGEVENS

16.1 X-Guard geeft geen Persoonsgegevens door aan een Niet Adequaat Land buiten de EER of enige Persoonsgegevens toegankelijk maken vanuit een Niet Adequaat Land zonder de vooraf verleende schriftelijke toestemming van Opdrachtgever.

16.2 Elke doorgifte van Persoonsgegevens aan een Derde in een Niet Adequaat Land zal worden beheerst door een overeenkomst conform de EU Modelcontractbepalingen. X-Guard garandeert dat Sub-Verwerkers die Opdrachtgever heeft goedgekeurd de desbetreffende overeenkomst conform de EU Modelcontractbepalingen mede-ondertekenen. X-Guard en Opdrachtgever zullen samenwerken om vergunningen, volmachten of toestemmingen aan te vragen en te verkrijgen die onder de AVG vereist zijn in verband met de uitvoering van dit Artikel 16.2.

16.3 Als in de loop van de Overeenkomst de EU-standaardcontractbepalingen (i) ongeldig worden verklaard door het Europese Hof van Justitie of (ii) worden vervangen door de Europese Commissie met een nieuwe of aangepaste standaardcontractbepalingen, zullen Opdrachtgever en X-Guard zonder onnodige vertraging te goeder trouw onderhandelen om dergelijke standaard contractuele clausules uit te voeren of een alternatief mechanisme voor gegevensoverdracht te implementeren dat wordt geboden door de toepasselijke wet op gegevensbescherming op schriftelijk verzoek van Opdrachtgever. Indien Opdrachtgever en X-Guard niet binnen twee maanden na de dag waarop Opdrachtgever een dergelijk schriftelijk verzoek heeft gedaan overeenstemming bereiken, heeft Opdrachtgever het recht om de Overeenkomst zonder kosten en met onmiddellijke ingang te beëindigen.

17 CONTACTPERSONEN

Alle kennisgevingen, bevestigingen en andere uitlatingen die Partijen hebben gedaan in verband met deze Bijlage worden schriftelijk gedaan en per aangetekende post en e-mail verzonden aan:

X-Guard BV
Welbergweg 50
7556 PE Hengelo
+31881261212

18 DEFINITIES

"AVG" betekent Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 April 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens;

"**Datalek**" betekent een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde Openbaring of verstrekking van of de ongeoorloofde toegang tot Persoonsgegevens;

"**Derde**" betekent eenieder die niet partij is bij de Overeenkomst;

"**EU Modelcontractbepalingen**" betekent de modelcontractbepalingen zoals gepubliceerd in het Besluit van de Europese Commissie van 5 februari 2010 (Besluit 2010/87/EC);

“**EER**” betekent alle lidstaten van de Europese Unie, Noorwegen, IJsland, Liechtenstein en (voor de toepassing van de Bijlage) Zwitserland;

"**Groepsmaatschappij**" betekent in verhouding tot ieder van partijen de uiteindelijke moedermaatschappij van die partij en ieder bedrijf, partnerschap of rechtspersoon waarin de uiteindelijke moedermaatschappij direct of indirect eigenaar is van meer van 50% van het geplaatste aandelenkapitaal of op andere wijze de activiteiten van dat bedrijf, partnerschap of rechtspersoon aanstuurt;

“**Individu**” betekent elke natuurlijke persoon wiens Persoonsgegevens worden Verwerkt door X-Guard ten behoeve van Opdrachtgever;

"**Medewerker**" betekent elke medewerker, agent, aannemer, oproepkracht of elke andere persoon die onder het directe gezag van X-Guard werkt;

“**Niet Adequaat Land**” betekent elk land dat niet wordt geacht een adequaat niveau van bescherming van Persoonsgegevens te hebben in de zin van de AVG;

“**Openbaarmaking**” betekent elke vorm van openbaar maken van Persoonsgegevens aan (inclusief toegang op afstand door) iedere Medewerker of onbevoegde Derde. "**Openbaren**” of “**Geopenbaard**” worden op dezelfde wijze gevormd;

"**Persoonsgegevens**" betekent elk gegeven betreffende een geïdentificeerd of identificeerbaar Individu;

"**Privacywetgeving**" betekent de AVG en alle wetten, regelgeving en sectorale richtlijnen die regels bevatten ter bescherming van individuen met betrekking tot de Verwerking, inclusief zonder beperking de beveiligingsvereisten voor en het vrij verkeer van Persoonsgegevens;

“**Sub-Verwerker**” betekent iedere derde die Persoonsgegevens Verwerkt onder instructie of toezicht van X-Guard maar die niet onder het directe gezag van X-Guard valt;

"Toepasselijke Verwerkerswetgeving" betekent de Privacywetgeving die van toepassing is op X-Guard als Verwerker;

“Toepasselijke Wetgeving” betekent de Privacywetgeving die van toepassing is op Opdrachtgever of X-Guard als Verwerkingsverantwoordelijken;

"**Verwerkingsverantwoordelijke**" betekent de onderneming of natuurlijke persoon die alleen of tezamen met anderen het doel van de Verwerking en de middelen daartoe bepaalt;

"**Verwerker**" betekent de onderneming of natuurlijke persoon die Persoonsgegevens verwerkt in opdracht van een Verwerkingsverantwoordelijke;

"**Verwerking**" betekent elke automatische of niet automatische activiteit die wordt uitgevoerd met betrekking tot Persoonsgegevens, zoals het verzamelen, vastleggen, opslaan, organiseren, wijzigen, gebruiken, openbaren, doorgeven of verwijderen van Persoonsgegevens. “**Verwerken**”, “**Verwerk**” of “**Verwerkt**” worden op dezelfde wijze gevormd.

Aldus in tweevoud opgemaakt en ondertekend:

Plaats:
Datum:

……	……
X-Guard B.V.	Opdrachtgever

APPENDIX I
SPECIFICATIE VAN VERWERKINGEN

In deze Appendix wordt een omschrijving gegeven van de Verwerkingen van Persoonsgegevens.

Omschrijving van de Verwerking:

In geval van agressie, geweld of calamiteit wordt er vanuit de Applicatie een alarmering Verwerkt en dit wordt doorgezet naar de alarmcentrale. Persoonsgegevens worden Verwerkt met als doel persoonsbeveiliging.

Categorieën van Persoonsgegevens, doeleinden en bewaartermijnen:

In de onderstaande tabel heeft X-Guard per Persoonsgegeven het doel van de Verwerking en de bewaartermijnen aangegeven. De Persoonsgegevens die gebruikt worden zijn de gegevens van de personen die X-Guard inzet bij de uitvoering van de Overeenkomst. Het algemeen doel van de Verwerking van de Persoonsgegevens is hulp en bijstand bieden aan persoon/klant die in noodsituatie verkeert.

Persoonsgegevens:	**Doeleinden:**	**Bewaartermijnen:**
Naam	Identificatie	contractduur
Adres Opdrachtgever	Identificatie klant	contractduur
Telefoonnummer	Om te kunnen communiceren	contractduur
Email adres	Om te kunnen communiceren	contractduur
Locatie Gebruiker	Identificatie van het alarm	1 maand
Gemaakt alarm	Hulp te kunnen bieden en te kunnen leren voor de toekomst	1 jaar
IPS locaties	t.b.v. locatiebepaling	Contractduur
Contactgegevens van opvolging	t.b.v. inzet van hulp/opvolging	Contractduur

Categorieën van betrokkenen:

Medewerkers van de Opdrachtgever en eventuele pnil'ers
Subverwerkers van X-Guard
Medewerkers van Opdrachtgever
Centralisten van de alarmcentrale

Categorieën medewerkers die Persoonsgegevens verwerken:

X-Guard maakt geen onderscheid in verschillende groepen van Medewerkers. Alle Medewerkers komen in aanraking met de Persoonsgegevens van medewerkers van Opdrachtgever (sales, aftersales, IT en administratie). Gezien de grootte van de onderneming is er geen specifiek onderscheid in toegang tot persoonsgegevens.

Sub-verwerkers:

1. PNIL'ers, o.a. zzp'ers die ingehuurd worden voor diverse specialismen.
2. Tellu, technologische partner voor dataverrijking.

Doorgiften:

Verwerkingsverantwoordelijke heeft Verwerker specifieke toestemming gegeven voor de hierna opgenomen doorgiften aan derde landen of internationale organisaties (in te vullen door Verwerkingsverantwoordelijke).

Beschrijving doorgifte	Entiteit die de Persoonsgegevens doorgeeft + land	Entiteit die de Persoonsgegevens ontvangt + land	Doorgifte-mechanisme

X-Guard geeft geen Persoonsgegevens door aan derde landen of internationale organisaties.

Ter verduidelijking onderstaande tabel:

		Categorieën persoons-gegevens Zet X indien ja								
Categorieën betrokkenen		Naam	Tel.nr	E-mail-adres	Actuele positie	Contact-personen	Adres	loginnaam	Doel(en)	Bewaar-termijn
Medewerkers (app-gebruikers)		x	x	x	x	x	x		Persoonsbeveiliging en communicatie	Contractduur
evt. PNIL (app gebruikers)		x	x	x	x	x	x		Persoonsbeveiliging en communicatie	Contractduur
Gebruikers (centralisten)		x		x				x	Persoonsbeveiliging en communicatie	Contractduur
Categorieën van ontvangers		Naam	Tel.nr	E-mail-adres	Actuele positie	Contact-personen	Adres		Doel(en)	Bewaar-termijn
Functioneel beheerder (Opdrachtgever)		x	x	x	x	x	x		Persoonsbeveiliging en communicatie	
Applicatiebeheerder (X-guard)		x	x	x	x	x	x		Persoonsbeveiliging en communicatie	
Centralisten (Alarmcentrale)		x	x	x	x	x	x		Persoonsbeveiliging en communicatie	
Externen: alarm opvolgers		x	x	x	x	x	x		Persoonsbeveiliging en communicatie	
technisch beheerder (X-guard / subverwerkers)		x	x	x	x	x	x		Persoonsbeveiliging en communicatie	

APPENDIX II

Informatiebeveiliging

1. Algemeen

Deze Appendix bevat eisen met betrekking tot risicomanagement en informatieveiligheid voor X-Guard en haar eventuele Sub-Verwerkers.

De versiedatum van deze Appendix is 26 januari 2022.

2. Introductie

Opdrachtgever heeft als doel betrouwbare producten, diensten en informatie aan haar klanten te leveren. Deze Appendix beschrijft de basiseisen die voor Opdrachtgever relevant zijn voor de beschikbaarheid, integriteit en vertrouwelijkheid van haar informatie. De maatregelen van X-Guard (en diens Sub-Verwerkers) dienen minimaal te voldoen aan de vereisten zoals beschreven in dit document.

Per eis geeft X-Guard aan of ze hieraan voldoet of op welke alternatieve wijze invulling is gegeven aan deze eis. In de toelichting kan per eis een onderbouwing van de beantwoording worden gegeven.

3. Informatieveiligheid en Risico Management

X-Guard voert tenminste éénmaal per jaar een risicoanalyse uit op al haar bedrijfsactiviteiten relevant voor de producten en/of diensten die aan Opdrachtgever geleverd worden. X-Guard geeft Opdrachtgever inzicht in de relevante resultaten van deze analyse. Indien X-Guard niet (meer) aan onderstaande vereisten voldoet en/of indien er sprake is van een gevaar voor de vertrouwelijkheid, integriteit of beschikbaarheid van de data van Opdrachtgever wordt Opdrachtgever op de hoogte gesteld. X-Guard zorgt ervoor dat de risico's worden gemitigeerd, in overeenstemming met Opdrachtgever, tot een aanvaardbaar tolerantieniveau.

4. IT Beheerprocessen

4.1 Continuitsbeheer

X-Guard heeft met betrekking tot continuïteitsbeheer proces en procedures beschreven en geborgd in haar organisatie. Er zijn actuele uitwijkplannen om bedrijfsactiviteiten tijdig te herstellen na onderbreking of verstoring van bedrijfskritieke en ondersteunende bedrijfsprocessen. Deze plannen omvatten naast uitwijk van ICT-voorzieningen ook maatregelen voor fysieke uitwijk.

X-Guard draagt er zorg voor en staat ervoor in dat:

- Taken, verantwoordelijkheden en bevoegdheden duidelijk zijn beschreven;
- Continuïteitsplannen actief beheerd en onderhouden worden;

- Jaarlijks de uitwijk van de ICT-voorzieningen, die zijn ingezet ten behoeve van de dienstverlening aan Opdrachtgever, wordt getest.

4.2 Wijzigingsbeheer

X-Guard heeft met betrekking tot wijzigingsbeheer processen en procedures beschreven en deze geborgd in haar organisatie.

X-Guard draagt er zorg voor en staat ervoor in dat:

- Een adequate scheiding tussen ontwikkel-, test-, acceptatie- en productieomgevingen is doorgevoerd;

- De ontwikkel-, test- en acceptatieomgevingen representatief zijn maar deze omgevingen bevatten geen productie dan wel persoonsgegevens in de zin van de Algemene Verordening Gegevensbescherming (AVG);

- Functiescheiding wordt toegepast waardoor wijzigingen gecontroleerd in productie worden doorgevoerd;

- Alle wijzigingen zijn beschreven en onderbouwd door middel van een audit-trail;

- Voor alle (kritieke) wijzigingen is een fallback scenario aanwezig.

X-Guard ontwikkelt nieuwe functionaliteit op basis van veiligheidsrichtlijnen die gebruikelijk zijn in de markt.

- X-Guard voert, ten minste voor iedere wijziging, code scans en/of 'reviews' uit op de broncode, om te waarborgen dat de broncode voldoet aan interne ontwikkelstandaarden en geen kwetsbaarheden bevat;

- Nieuwe releases van internet facing webapplicaties worden onderworpen aan een security test (penetratie test).

4.3 Datamanagement

X-Guard heeft processen en procedures beschreven en deze geborgd in haar organisatie om data van Opdrachtgever veilig op te slaan, te verwerken en te archiveren. Dit met als doel om te voldoen aan business doelstellingen, wet- en regelgeving en (IT-) securitybeleid. Opdrachtgever blijft te allen tijde eigenaar van de Opdrachtgevers-data en -logging ten aanzien van de afgenomen diensten door Opdrachtgever.

X-Guard conformeert zich aan de volgende eisen met betrekking tot datamanagement:

- X-Guard garandeert dat Opdrachtgevers-data (inclusief kopieën en back-ups) niet worden opgeslagen, verwerkt of gearchiveerd buiten de Europese Economische Ruimte;

- Bij verwijdering of vervanging van een medium waar Opdrachtgeversdata op staat wordt deze adequaat vernietigd, zodat de data op geen enkele manier te herstellen valt;

- Alle voor de uitbestede product of dienst gebruikte informatiesystemen zijn ondergebracht in datacenters met een ISO 27001 of vergelijkbare certificering;

- Voor alle door X-Guard beheerde websites wordt periodiek een scan op kwetsbaarheden uitgevoerd en bevindingen worden adequaat opgelost;

- X-Guard versleutelt (/encrypt) essentiële Opdrachtgeversdata tijdens het transport over onbeveiligde netwerken. Versleuteling dient te voldoen aan de richtlijn van het NCSC voor Transport Layer Security (TLS). De aspecten authenticiteit, bewijs van afgifte, bewijs van ontvangst en non-repudiation van oorsprong worden door X-Guard gegarandeerd.

X-Guard maakt regelmatig back-ups van essentiële informatie, waarbij

- De back-ups veilig en op veilige afstand worden bewaard;

- Het back-up en herstelproces regelmatig wordt getest op goede werking;

- De rapportages hieromtrent voor Opdrachtgever beschikbaar zijn.

4.4 Securitymanagement

X-Guard monitort en test op een proactieve manier haar IT-infrastructuur om de (industry best practice) security baselines te handhaven.

- X-Guard is in staat om cybercrime aanvallen te detecteren en hierop adequaat te reageren en te handelen waardoor schade voor Opdrachtgever wordt beperkt tot een minimum;

- X-Guard beschermt logging gegevens tegen ongewenst wijzigen of in zien;

- X-Guard treft maatregelen voor detectie, preventie en herstel om te beschermen tegen malware. X-Guard traint haar medewerkers regelmatig om de risico's van malware te verkleinen en het bewustzijn omtrent de schadelijke gevolgen van malware bij deze medewerkers te vergroten;

- X-Guard heeft een actief kwetsbaarhedenbeheerproces dat (security)patches test en tijdig doorvoert op de informatiesystemen;

- Kritische handelingen van gebruikers- en beheerders op netwerk-, besturingssysteem- en databaseniveau worden gelogged en niet-reguliere handelingen worden gesignaleerd

4.5 Accessmanagement

X-Guard heeft een proces voor logische toegangsbeveiliging beschreven en geborgd in de organisatie. X-Guard draagt er zorg voor en staat ervoor in dat:

- Er procedures bestaan ten aanzien van het toekennen, wijzigen en intrekken van autorisaties voor de toegang tot systemen waarop informatie van Opdrachtgever wordt verwerkt. De autorisaties moeten gebaseerd zijn op gedefinieerde profielen en moeten in lijn zijn met de geldende functiescheiding;

- Alle gebruikers (intern, extern en tijdelijk) uniek identificeerbaar zijn op de IT-systemen (business applicatie en onderliggende IT-infrastructuur);

- De autorisaties direct worden aangepast bij wijzigingen, zoals uitdiensttreding, overplaatsing of functiewijziging van betreffende medewerkers;

- Door verwerker wordt een wachtwoord beleid gevoerd waarbij gebruik gemaakt wordt van twee factoren tbv authenticatie. Wachtwoorden kunnen voor een periode van 12 maanden niet worden hergebruikt.

- Het maximumaantal toegestane pogingen tot aanloggen is beperkt tot 3;

- De gebruikersaccounts (user-id's) dienen steeds persoonlijk te zijn, zodat gebruikers uitsluitend onder eigen account werken;

- Een audit trail wordt vastgelegd met daarin aanlogpogingen, de melding van foute aanlogpogingen en het signaleren en afhandelen van aanlogincidenten.