Verwerkersovereenkomst

DE ONDERGETEKENDEN:

1. Het Nederlands Diensten Centrum voor ICT (NDC-IT), statutair gevestigd Hoorn en kantoorhoudend te (1505HH) Zaandam aan de Vredeweg 1V, ingeschreven in het register van de Kamer van Koophandel onder nummer 37160577, hierbij rechtsgeldig vertegenwoordigd door J. Budde, hierna te noemen "**Verwerker**";

2. [Naam Verwerker], statutair gevestigd en kantoorhoudend te gevestigd te [(postcode)] [plaats] aan [adres en nummer]en ingeschreven in het register van de Kamer van Koophandel onder nummer [KvK-nummer], hierbij rechtsgeldig vertegenwoordigd door [invullen], hierna te noemen "**Verwerkingsverantwoordelijke**".

   Hierna gezamenlijk ook aan te duiden als: "Partijen" en afzonderlijk als "Partij".

VERKLAREN TE ZIJN OVEREENGEKOMEN ALS VOLGT:

Artikel 1. Onderwerp van deze Verwerkersovereenkomst

1.1 Deze Verwerkersovereenkomst (hierna: "**Verwerkersovereenkomst**") is exclusief van toepassing op het verwerken van persoonsgegevens in het kader van de overeenkomst [naam overeenkomst] van [datum] tussen Partijen voor de uitvoering van overeengekomen diensten (hierna: "**Overeenkomst**").

1.2 Begrippen uit de Algemene Verordening Gegevensbescherming (EU) 2016/679 (hierna: "**AVG**") zoals: "**betrokkenen**", "**persoonsgegevens**", "**verwerking**", "**Verwerker**", "**Verwerkingsverantwoordelijke**" hebben de betekenis die daaraan is gegeven in de AVG.

1.3 Verwerker kan gedurende de uitvoering van de in de Overeenkomst genoemde diensten ten behoeve van Verwerkingsverantwoordelijke persoonsgegevens verwerken. Een overzicht van de categorieën persoonsgegevens, de doeleinden waarvoor de persoonsgegevens worden verwerkt en een omschrijving van de verwerking(en) zijn opgenomen in **Annex 1** bij deze Verwerkersovereenkomst.

Artikel 2. De Verwerkingsverantwoordelijke en de Verwerker

2.1 De Verwerker zal optreden als Verwerker en de Verwerkingsverantwoordelijke zal optreden als Verwerkingsverantwoordelijke.

2.2 Verwerker garandeert dat hij ten behoeve van Verwerkingsverantwoordelijke uitsluitend persoonsgegevens zal verwerken op een wijze die - en voor zover dit - noodzakelijk is voor de levering van de prestaties onder de in artikel 1 van deze Verwerkersovereenkomst genoemde Overeenkomst. Overige verwerkingen zullen uitsluitend worden uitgevoerd in expliciete opdracht van Verwerkingsverantwoordelijke of als daartoe een wettelijke verplichting bestaat. In geen geval zal Verwerker persoonsgegevens verwerken voor eigen doeleinden.

2.3 Verwerker zal alle redelijke schriftelijke instructies van Verwerkingsverantwoordelijke in verband met de verwerking van de persoonsgegevens opvolgen. Verwerker stelt Verwerkingsverantwoordelijke onmiddellijk op de hoogte indien naar zijn oordeel instructies in strijd zijn met de toepasselijke wetgeving met betrekking tot de verwerking van persoonsgegevens of met een tussen partijen geldende overeenkomst.

2.4 Verwerker zal de persoonsgegevens op behoorlijke en zorgvuldige wijze en in overeenstemming met toepasselijke wetgeving met betrekking tot de verwerking van persoonsgegevens verwerken, waarbij in elk geval tot 18 mei 2018 de Wet bescherming persoonsgegevens (hierna: "**Wbp**") geldt en vanaf 25 mei 2018 de AVG. Partijen sluiten de overeenkomst om te profiteren van de expertise die Verwerker heeft als het gaat om het verwerken van Persoonsgegevens voor de doeleinden die uiteengezet zijn in **Annex 1** bij deze Verwerkersovereenkomst. Het is Verwerker toegestaan om naar eigen inzicht de middelen aan te wenden die hij noodzakelijk acht om die doeleinden na te streven.

2.5 Verwerker zal geen persoonsgegevens doorgeven aan landen buiten de Europese Economische Ruimte ("**EER**") zonder een passend beschermingsniveau, tenzij:

a. Verwerker hiervoor uitdrukkelijke voorafgaande schriftelijke toestemming heeft verkregen van Verwerkingsverantwoordelijke en voldaan wordt aan alle wettelijke vereisten. Verwerkingsverantwoordelijke heeft te allen tijde het recht om aanvullende voorwaarden te verbinden aan zijn toestemming voor een dergelijke verwerking; of
b. een op de Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot verwerking verplicht. In dat geval stelt de Verwerker de in **Annex 2** genoemde medewerker van Verwerkingsverantwoordelijke, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

2.6 Onverminderd enige andere contractuele geheimhoudingverplichting die op Verwerker rust, garandeert Verwerker dat hij alle persoonsgegevens als strikt vertrouwelijk zal behandelen en dat hij al zijn werknemers, vertegenwoordigers en/of subverwerkers die betrokken zijn bij de verwerking van de Persoonsgegevens van de vertrouwelijke aard van dergelijke informatie en van de persoonsgegevens op de hoogte zal stellen. Verwerker zal waarborgen dat dergelijke personen en partijen een adequate geheimhoudingsovereenkomst hebben getekend en dat zij zich houden aan de bepalingen van deze Verwerkersovereenkomst en zal Verwerkingsverantwoordelijke op verzoek van kopieën van deze overeenkomsten voorzien. Het is Verwerker niet toegestaan de Persoonsgegevens aan enige derde te tonen, verstrekken of anderszins ter beschikking te stellen, tenzij dit noodzakelijk of toegestaan is ingevolge de opdracht zoals neergelegd in de Overeenkomst of in het geval hiervoor expliciete voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke is verkregen.

2.7 Verwerker zal zijn volledige medewerking verlenen aan Verwerkingsverantwoordelijke om (i) na goedkeuring van en in opdracht van Verwerkingsverantwoordelijke betrokkenen toegang te laten krijgen tot de hun betreffende persoonsgegevens, (ii) persoonsgegevens te verwijderen of te corrigeren, (iii) aan te tonen dat persoonsgegevens verwijderd of gecorrigeerd zijn indien zij incorrect zijn (of, ingeval Verwerkingsverantwoordelijke het er niet mee eens is dat persoonsgegevens incorrect zijn, het feit vast te leggen dat de betrokkene zijn persoonsgegevens als incorrect beschouwt) en (iv) Verwerkingsverantwoordelijke anderszins in de gelegenheid te stellen om aan zijn verplichtingen onder de WBP en vanaf 25 mei 2018 de AVG en andere toepasselijke wetgeving met betrekking tot de verwerking van persoonsgegevens te voldoen.

2.8 Verwerker zal de persoonsgegevens betreffende Verwerkingsverantwoordelijke strikt gescheiden opslaan en verwerken van de persoonsgegevens die zij voor zichzelf of namens derde partijen verwerkt.

Artikel 3. Beveiliging persoonsgegevens en controle

3.1 Onverminderd de beveiligingsnormen die Partijen elders zijn overeengekomen, zal Verwerker passende technische en organisatorische beveiligingsmaatregelen nemen, rekening houdend met de stand van de techniek, de uitvoeringskosten, 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, ter bescherming van de persoonsgegevens tegen vernietiging, verlies, wijziging, ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig. Deze maatregelen omvatten in ieder geval:

(a) maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de persoonsgegevens voor de doeleinden die zijn uiteengezet in **Annex 3**;

(b) maatregelen om de persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag verwerking, toegang of openbaarmaking;

(c) maatregelen om zwakke plekken te identificeren ten aanzien van de verwerking van persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan Verwerkingsverantwoordelijke;

(d) de maatregelen die Partijen in Annex 3 zijn overeengekomen.

3.2 Verwerker heeft te allen tijde een passend, geschreven beveiligingsbeleid geïmplementeerd voor de verwerking van persoonsgegevens, waarin in ieder geval de in artikel 3.1 genoemde maatregelen uiteen zijn gezet.

3.3 Verwerkingsverantwoordelijke heeft het recht toe te zien op de naleving van de hiervoor onder artikel 3.1 en 3.2 genoemde maatregelen. Verwerker stelt Verwerkingsverantwoordelijke, indien Verwerkingsverantwoordelijke daarom verzoekt, hiertoe in elk geval eenmaal per jaar in de gelegenheid op een door Partijen in gezamenlijk overleg nader te bepalen tijdstip en verder indien Verwerkingsverantwoordelijke daar aanleiding toe ziet naar aanleiding van (vermoeden van) informatie- of privacy-incidenten. Verwerker zal eventuele door Verwerkingsverantwoordelijke naar aanleiding van een dergelijke controle in redelijkheid gegeven instructies tot aanpassing van het beveiligingsbeleid binnen een redelijke termijn opvolgen.

3.4 Verwerker zal in alle redelijkheid en op eigen kosten aan het in artikel 3.3 bedoelde onderzoek zijn medewerking verlenen.

3.5 Partijen erkennen dat beveiligingseisen voortdurend veranderen en dat een effectieve beveiliging frequente evaluatie en regelmatige verbetering van verouderde beveiligingsmaatregelen vereist. Verwerker zal daarom de maatregelen zoals geïmplementeerd op basis van dit artikel 3 voortdurend evalueren en verscherpen, aanvullen of verbeteren om te blijven voldoen aan zijn verplichtingen onder dit artikel 3.

Artikel 4. Monitoring, informatieplichten en incidentenmanagement

4.1 Verwerker zal actief monitoren op inbreuken op de beveiligingsmaatregelen en over de resultaten van de monitoring in overeenstemming met dit artikel 4 rapporteren aan Verwerkingsverantwoordelijke binnen de daarvoor gestelde wettelijke termijnen.

4.2 Zodra zich een incident met betrekking tot de verwerking van de persoonsgegevens voordoet, heeft voorgedaan of zou kunnen voordoen met betrekking tot beveiligingsmaatregelen, is Verwerker verplicht Verwerkingsverantwoordelijke daarvan onverwijld in kennis te stellen en daarbij alle relevante informatie te verstrekken omtrent de aard van het incident, het risico dat gegevens onrechtmatig verwerkt zijn of kunnen worden en de maatregelen die getroffen zijn of zullen worden om het incident op te lossen dan wel de gevolgen/schade zoveel mogelijk te beperken.

4.3 Verwerker zal Verwerkingsverantwoordelijke te allen tijde zijn medewerking verlenen en zal de instructies van Verwerkingsverantwoordelijke opvolgen, met als doel Verwerkingsverantwoordelijke in staat te stellen een deugdelijk onderzoek te verrichten naar het incident, een correcte respons te formuleren en passende vervolgstappen te nemen ten aanzien van het incident.

4.4 Onder "**incident**" wordt in elk geval het volgende verstaan:

(a) een klacht of (informatie)verzoek van een natuurlijk persoon met betrekking tot de verwerking van persoonsgegevens door Verwerker;

(b) een onderzoek naar of beslaglegging door overheidsfunctionarissen op de persoonsgegevens of een vermoeden dat dit gaat plaatsvinden, tenzij het Verwerker wettelijk niet is toegestaan hiervan melding te doen aan Verwerkingsverantwoordelijke;

(c) iedere ongeautoriseerde toegang, verwerking, verwijdering, verlies of enige vorm van onrechtmatige verwerking van de persoonsgegevens;

(d) een doorbreking van de beveiliging en/of de vertrouwelijkheid, zoals uiteengezet in artikel 3 en 4 van deze Verwerkersovereenkomst, die leidt tot onopzettelijke of onrechtmatige vernietiging, verlies, wijziging, onbevoegde openbaarmaking van – of toegang tot – de persoonsgegevens, of enige aanwijzing dat een dergelijke inbreuk zal plaatsvinden of heeft plaatsgevonden.

4.5 Verwerker zal te allen tijde geschreven procedures voorhanden hebben die hem in staat stellen om Verwerkingsverantwoordelijke van een onmiddellijke reactie over een incident te voorzien, en om effectief samen te werken met Verwerkingsverantwoordelijke om het incident af te handelen en zal Verwerkingsverantwoordelijke voorzien van een exemplaar van dergelijke procedures indien Verwerkingsverantwoordelijke daarom verzoekt.

4.6 Meldingen die worden gedaan op grond van dit artikel worden gericht aan de in Annex 2 opgenomen werknemer van Verwerkingsverantwoordelijke of, indien relevant, aan een andere door Verwerkingsverantwoordelijke tijdens de duur van deze Verwerkersovereenkomst schriftelijk bekendgemaakte andere werknemer van Verwerkingsverantwoordelijke.

4.7 Verwerkingsverantwoordelijke zal, indien naar zijn oordeel noodzakelijk, betrokkenen, toezichthouders en andere derden informeren over incidenten. Het is Verwerker niet toegestaan informatie te verstrekken over incidenten aan betrokkenen of andere derde partijen, behoudens voor zover Verwerker daartoe wettelijk verplicht is.

Artikel 5. Gebruik onderaannemers

5.1 Verwerker zal zijn activiteiten die (deels) bestaan uit het verwerken van persoonsgegevens of vereisen dat persoonsgegevens verwerkt worden niet uitbesteden aan een derde partij ("**subverwerker**") zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke.

5.2 Verwerker zal aan de door hem ingeschakelde subverwerker dezelfde of strengere verplichtingen opleggen als voor hemzelf uit deze Verwerkersovereenkomst en de wet voortvloeien en ziet toe op de naleving daarvan door de derde.

5.3 Niettegenstaande de toestemming van Verwerkingsverantwoordelijke voor het inschakelen van een derde partij blijft Verwerker volledig aansprakelijk jegens Verwerkingsverantwoordelijke voor de gevolgen van het uitbesteden van werkzaamheden aan een subverwerker. De toestemming van Verwerkingsverantwoordelijke voor het uitbesteden van werkzaamheden aan een subverwerker laat onverlet dat voor de inzet van subverwerkers in een land buiten de EER zonder een passend beschermingsniveau toestemming vereist is in overeenstemming met artikel 2.5 van deze Verwerkersovereenkomst.

Artikel 6. Vrijwaring

6.1 Verwerker vrijwaart Verwerkingsverantwoordelijke en stelt Verwerkingsverantwoordelijke schadeloos voor alle claims, acties, aanspraken van derden en voor verliezen, schade of kosten, waaronder boetes en dwangsommen van de Autoriteit Persoonsgegevens, die Verwerkingsverantwoordelijke lijdt of maakt en die rechtstreeks of indirect voortvloeien uit of tot stand komen in verband met een tekortkoming door Verwerker of subverwerker in de nakoming van zijn verplichtingen onder deze Verwerkersovereenkomst en/of enige schending door Verwerker of subverwerker van de van toepassing zijnde wetgeving op het gebied van verwerking van persoonsgegevens in verband met de Overeenkomst, waaronder in elk geval de WBP en vanaf 25 mei 2018 de AVG.

6.2 De vergoeding die Verwerker aan Verwerkingsverantwoordelijke verschuldigd is op basis van artikel 6.1, is beperkt tot € 10.000 per gebeurtenis. Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis. De beperking in aansprakelijkheid dient van geval van tot geval te worden beoordeeld en te worden afgestemd met een jurist van de NDC-IT. De maximale aansprakelijkheid is in ieder geval afhankelijk van de aard van de prestatie, de daaraan verbonden risico's en de omvang van de vergoeding.

Artikel 7. Duur en beëindiging

7.1 Deze Verwerkersovereenkomst gaat in op [datum] en geldt voor de duur van de Overeenkomst.

7.2 Verplichtingen welke naar hun aard bestemd zijn om ook na beëindiging van deze Verwerkersovereenkomst voort te duren, blijven na beëindiging van de Verwerkersovereenkomst gelden. Tot deze bepalingen behoren onder meer die welke voortvloeien uit de bepalingen betreffende geheimhouding, aansprakelijkheid en toepasselijk recht.

Artikel 8. Bewaartermijnen, teruggave en vernietiging van Persoonsgegevens

8.1 Verwerker bewaart de persoonsgegevens niet langer dan strikt noodzakelijk en in geen geval langer dan tot het einde van deze Verwerkersovereenkomst of, indien tussen partijen een bewaartermijn is overeengekomen, niet langer dan deze termijn.

8.2 Bij beëindiging van deze Verwerkersovereenkomst, of indien van toepassing aan het einde van de overeengekomen bewaartermijnen, of op schriftelijk verzoek van Verwerkingsverantwoordelijke, zal Verwerker de persoonsgegevens vernietigen of teruggeven aan Verwerkingsverantwoordelijke, naargelang de keuze van Verwerkingsverantwoordelijke, tenzij opslag van de persoonsgegevens op basis van toepasselijk Unierecht of lidstatelijk recht verplicht is. Op verzoek van Verwerkingsverantwoordelijke verstrekt Verwerker bewijs van het feit dat de gegevens vernietigd of verwijderd zijn.

8.3 Bij het einde van de Verwerkersovereenkomst zal Verwerker alle derden die betrokken zijn bij het verwerken van persoonsgegevens op de hoogte stellen van de beëindiging van de Verwerkersovereenkomst en zal waarborgen dat alle betrokken derden de persoonsgegevens vernietigen of aan Verwerkingsverantwoordelijke overdragen, naar keuze van Verwerkingsverantwoordelijke.

Artikel 9. Slotbepalingen

9.1 In het geval van strijdigheid tussen de bepalingen uit deze Verwerkersovereenkomst en bepalingen uit de Overeenkomst, dan zullen de bepalingen van de Verwerkersovereenkomst leidend zijn.

9.2 Op deze Verwerkersovereenkomst zijn de bepalingen van de is Nederlands recht van toepassing. Geschillen over of in verband met deze Verwerkersovereenkomst worden uitsluitend voorgelegd aan de bevoegde rechter in Amsterdam.

Nederlands Diensten Centrum voor ICT	[naam Verwerker]
Plaats: Zaandam	Plaats: .....
Datum:	Datum: .....
_____	_____
[J. Budde]	[Naam vertegenwoordiger Verwerker]
[Directeur]	[Functie]

ANNEX 1: Te verwerken persoonsgegevens, doeleinden en omschrijving verwerking(en)

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.

Beschrijving Verwerkingsactiviteiten door verwerker:	
Verwerkingsdoelen:	
Verwerkingsverantwoordelijke:	
Verwerker:	
Sub verwerkers:	
Verwerkte persoonsgegevens:	
Locatie verwerkingen:	
Bewaartermijn:	

ANNEX 2: Contactgegevens

[Invoegen contactgegevens medewerker Verwerkingsverantwoordelijke waarmee contact dient te worden opgenomen in het geval van "incidenten"/datalekken]

NAAM:	Functie:	Telefoon:	Email:

ANNEX 3: Beveiligingsmaatregelen

Hier moet een overzicht van de beveiligingsnormen opgenomen worden die de Verwerkingsverantwoordelijke aan de Verwerker opgelegd. Om vast te stellen wat passende beveiligingsmaatregelen zijn moet 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 emailadres, wat minder gevoelige persoonsgegevens zijn, of gaat het om het verwerken van een BSN.*
- De hoeveelheid betrokkenen van wie gegevens worden verwerkt. *Hoe meer betrokkenen er zijn hoe meer eisen er worden gesteld aan de beveiliging van de gegevens.*
- Het doel waarvoor gegevens worden verwerkt.
- De duur en de wijze waarop gegevens bewaard moeten worden. Er kan vervolgens onderscheid gemaakt worden tussen organisatorische beveiligingseisen, zoals het voorkomen van diefstal van een laptop met daarop persoonsgegevens uit de auto, en technische beveiligingseisen, zoals een uitgebreide IT omgeving die beveiligd wordt tegen virussen en waar encryptie van de gegevens wordt toegepast. Van een grote organisatie wordt meer verwacht ten aanzien van de te nemen beveiligingseisen.

Technische beveiligingsmaatregelen

☑ Up to date virusscan
☐ Beveiligde USB-sticks
☐ Accurate beveiliging medewerkerstelefoon
☑ Bitlocker toegangsmechanisme
☑ Unieke inlogcode en wachtwoord (regelmatig aanpassen)
☐ Versleutelde email
☑ Geen onbeveiligde externe harde schijven
☑ Geen onbeveiligde back-ups maken
☐ Geen documenten op privé laptop op slaan

Organisatorische beveiligingsmaatregelen

☐ Clean desk policy
☐ Laptop niet onbemand achterlaten
☐ Laptop nooit achterlaten in de auto
☐ Oude documenten op juiste manier vernietigen
☐ Zorgvuldig gebruik van USB-sticks

ANNEX 4: Proces rondom het melden van Datalekken en de te verstrekken informatie

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, log in gegevens, cookies, IP adressen of identificerende gegevens van computers of telefoons.

Hieronder vind je een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de Autoriteit Persoonsgegevens.

- De website met logingegevens is gehackt of is toegankelijk voor derden.
- Verlies van een laptop of USB-stick met persoonsgegevens.
- Salarisstroken van medewerkers zijn per ongeluk naar verkeerde personen gestuurd.
- Brieven of e-mails worden naar een verkeerd adres gestuurd.
- Een aanval van een hacker op het ICT systeem.
- Een verloren of gestolen telefoon waar persoonsgegevens op aanwezig zijn.

<u>Wat te doen bij twijfel?</u>
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

NAAM: _____

<u>Waar meld je het beveiligingsincident?</u>
Als je een beveiligingsincident hebt ontdekt, neem je direct contact op met de

NAAM: _____

TEL: _____

Of

E-MAIL: _____

<u>Geef in je e-mail beantwoording op de onderstaande vragen.</u>

1. Geef een samenvatting van het beveiligingslek / beveiligingsincident / datalek: wat is er gebeurd? Vermeld hier ook de naam van het betrokken systeem.

2. Welke typen persoonsgegevens zijn betrokken bij het beveiligingsincident?
   Zoals, maar niet beperkt tot, naam, adres, e-mailadres, IP-nummer, Burgerservicenummer, pasfoto en ieder ander tot een persoon te herleiden gegeven.

3. Van hoeveel personen zijn de persoonsgegevens betrokken bij het beveiligingsincident?
   Geef a.u.b. een minimum en maximum aantal personen.

4. Omschrijving groep personen om wiens gegevens het gaat.
   Geef aan of het gaat om medewerkersgegevens, gegevens van internetgebruikers. Bijzondere aandacht verdienen gegevens van een kwetsbare groepen personen, zoals kinderen.

5. Zijn de contactgegevens van de betrokken personen bekend?
   Het kan zijn dat betrokkenen geïnformeerd moeten worden over het datalek, kunnen we deze personen in dat geval bereiken?

6. Wat is de oorzaak (root cause) van het beveiligingsincident?
   Heeft u een idee hoe het beveiligingsincident heeft kunnen ontstaan?

7. Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden?
   Geef dit a.u.b. zo specifiek mogelijk aan.