

Concept Verwerkersovereenkomst

Verwerkersovereenkomst [NAAM LEVERANCIER]

Contractpartijen:

1. Verwerkingsverantwoordelijke te weten Stichting het Juridisch Loket, statutair gevestigd te Moreelsepark 1 (3e etage) 3511 EP Utrecht, rechtsgeldig vertegenwoordigd door R.J.W.G Janssen, hierna te noemen: '**Verwerkingsverantwoordelijke**',
en
2. Verwerker te weten [STATUTAIRE NAAM], statutair gevestigd te [PLAATS], rechtsgeldig vertegenwoordigd door [NAAM EN/OF NAAM TEKENBEVOEGDE BESTUURDER], hierna te noemen: '**Verwerker**',

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

Overwegende dat:

- Partijen een Contract hebben gesloten met betrekking tot Mobiele Telefonie Ter uitvoering van dit Contract worden Persoonsgegevens verwerkt.
- Verwerkingsverantwoordelijke grote waarde hecht aan het beschermen van deze Persoonsgegevens. Om die reden leggen Partijen in deze Verwerkersovereenkomst en de daarbij behorende annexen, te weten:
 - a. overzicht met verwerkingen van Persoonsgegevens en verwerkingsdoelen;
 - b. overzicht met beveiligingsmaatregelen;
 - c. proces rondom het melden van Datalekken en de te verstrekken informatie met betrekking tot het Datalek;vast wat Verwerker wel en niet mag doen met de Persoonsgegevens.

1. Definities

De hierna en hiervoor gebruikte begrippen volgen uit de Algemene Verordening Gegevensbescherming en hebben de volgende betekenis:

- 1.1 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('**de Betrokkene**'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identicator zoals een naam, een identificatienummer, locatiegegevens, een online identicator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon, die Verwerker in het kader van het Contract ten behoeve van Verantwoordelijke verwerkt. Dit is niet beperkt tot de inhoudelijke persoonsgegevens die Verantwoordelijke actief aan (het systeem van) Verwerker verstrekt, maar omvat ook de persoonsgegevens die Verwerker genereert en verwerkt over het

- gebruik van het systeem/de diensten (Diagnostische gegevens), en gegevens die Verwerker genereert en verwerkt in algemene security logs.
- 1.2 Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
 - 1.3 Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van Persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijk recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen (**'Verwerkingsverantwoordelijke'**).
 - 1.4 Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke Persoonsgegevens verwerkt (**'Verwerker'**).
 - 1.5 Sub-verwerker: een partij die namens de Verwerker persoonsgegevens verwerkt voor de Verwerkingsverantwoordelijke.
 - 1.6 Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte Persoonsgegevens betrekking hebben.
 - 1.7 Verwerkersovereenkomst: deze overeenkomst inclusief de annexen (**'Verwerkersovereenkomst'**).
 - 1.8 Contract: het hoofdcontract waar deze Verwerkersovereenkomst uit voortvloeit.
 - 1.9 Inbreuk in verband met Persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens (**'Datalek'**).
 - 1.10 Gegevensbeschermingseffectbeoordeling: het uitvoeren van een beoordeling, voorafgaand aan het uitvoeren van de verwerking, van het effect van de beoogde verwerkingsactiviteiten op de bescherming van de persoonsgegevens.
 - 1.11 Toezichthouder: een onafhankelijke overheidsinstantie verantwoordelijk voor het toezicht op de naleving van de wet in verband met de verwerking van Persoonsgegevens. In Nederland is dit de Autoriteit Persoonsgegevens.

Artikel 2. Doel van deze Verwerkersovereenkomst

- 2.1 Deze Verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Verwerker in het kader van het Contract.
- 2.2 De aard en het doel van de Verwerking, welke Persoonsgegevens Verwerker precies zal verwerken en voor welke verwerkingsdoeleinden, Betrokkenen en ontvangers zijn in Annex 1 omschreven.

Artikel 3. Verplichtingen van de Verwerker

- 3.1 Verwerker verwerkt de Persoonsgegevens slechts in overleg met Verantwoordelijke, behoudens afwijkende wettelijke verplichtingen. Verwerker verwerkt Persoonsgegevens overeenkomstig schriftelijke instructies van Verantwoordelijke en onder diens verantwoordelijkheid en mag de Persoonsgegevens niet op een andere manier verwerken, tenzij Verwerkingsverantwoordelijke Verwerker daar van tevoren toestemming of opdracht voor geeft.
- 3.2 De Verwerker stelt de Verwerkingsverantwoordelijke onverwijld in kennis indien, naar het oordeel van de Verwerker, door de Verwerkingsverantwoordelijke gegeven instructies in strijd zijn met de Algemene Verordening Gegevensbescherming en/of andere relevante privacy wetgeving.
- 3.3 De Persoonsgegevens door Verwerker verwerkt blijven uitsluitend eigendom van Verantwoordelijke.
- 3.4 De Verwerker neemt geen zelfstandige beslissingen over het verwerken van de Persoonsgegevens voor andere doeleinden, waaronder over de verstrekking daarvan aan derden en de duur van de opslag van gegevens. De zeggenschap over Persoonsgegevens verstrekt aan Verwerker in het kader van het Contract, alsmede over de door Verwerker in dat kader verwerkte gegevens, berust bij Verantwoordelijke.
- 3.5 Verwerker garandeert de toepassing van passende technische en organisatorische maatregelen zoals nader toegelicht in artikel 7 en Annex 2, opdat de Verwerking aan de vereisten van de Algemene Verordening Gegevensbescherming voldoet en de bescherming van de rechten van de Betrokkene is gewaarborgd.
- 3.6 Verwerker garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens en aan toepasselijke ePrivacy regelgeving, inclusief de Electronic Communications Code.
- 3.7 Wanneer Verwerkingsverantwoordelijke een verzoek van een Betrokkene ontvangt ten aanzien van het uitoefenen van zijn of haar rechten, dan werkt Verwerker daar aan mee door binnen een termijn van 14 dagen inhoudelijk te antwoorden. Deze rechten bestaan uit een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming, bezwaar maken tegen de verwerking van de Persoonsgegevens en een verzoek tot overdraagbaarheid van de eigen Persoonsgegevens. Verwerker verleent Verantwoordelijk zoveel mogelijk directe inzage in alle verwerkte Persoonsgegevens via een digitale interface, waaronder inzage in de Diagnostische Gegevens.
- 3.8 Een door Verwerker ontvangen verzoek van een Betrokkene met betrekking tot verwerking van Persoonsgegevens wordt door Verwerker zonder uitstel, maar in ieder geval binnen 2 werkdagen, doorgestuurd naar Verantwoordelijke.

4. Totstandkoming, duur en beëindiging van deze Verwerkersovereenkomst

- 4.1 Deze Verwerkersovereenkomst treedt in werking op de datum waarop Partijen deze ondertekenen.
- 4.2 Deze Verwerkersovereenkomst is onderdeel van het Contract en zal gelden voor zolang het Contract duurt.
- 4.3 Indien het Contract eindigt, eindigt deze Verwerkersovereenkomst automatisch; de

Verwerkersovereenkomst kan niet apart of tussentijds worden opgezegd.

- 4.4 Na beëindiging van deze Verwerkersovereenkomst zullen de lopende verplichtingen voor Verwerker, zoals het melden van Datalekken waarbij Persoonsgegevens van Verwerkingsverantwoordelijke betrokken zijn en de plicht tot geheimhouding blijven voortduren.

5. Inschakelen van sub-verwerkers

- 5.1 Verwerker mag zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke geen andere partijen of organisaties ('**sub-verwerkers**') inschakelen bij het verwerken van de Persoonsgegevens.
- 5.2 Wanneer Verwerker met toestemming van Verwerkingsverantwoordelijke andere partijen of organisaties inschakelt, zorgt Verwerker er voor dat aan de ingeschakelde sub-verwerker dezelfde verplichtingen worden opgelegd als aan Verwerker door Verantwoordelijke. Verwerker blijft jegens Verantwoordelijke volledig aansprakelijk voor het nakomen van de verplichtingen door de sub-verwerker.
- 5.3 Verantwoordelijke gaat akkoord met het inschakelen van de specifieke sub-verwerkers opgesomd in Annex 1, telkens met aanduiding van de soorten persoonsgegevens en de doelen waarvoor de sub-verwerker wordt ingeschakeld.
- 5.4 Verwerker zal geen sub-verwerkers buiten de "EER" inschakelen en ook niet toestaan dat haar sub-verwerkers sub-subverwerkers inschakelen buiten de EER (Europese Economische Ruimte).
- 5.5 Wanneer Verwerker voornemens is een nieuwe sub-verwerker in te schakelen zal Verwerker Verantwoordelijke hierover in beginsel 60 werkdagen van tevoren informeren. Verantwoordelijke heeft vervolgens 15 werkdagen het recht schriftelijk bezwaar te maken tegen een verandering. Indien er geen bezwaar is ingediend binnen de opgegeven termijn wordt aangenomen dat de Verantwoordelijke akkoord is gegaan met de verandering van de sub-verwerker. Verwerker zal de Persoonsgegevens van Verantwoordelijke niet door de nieuwe sub-verwerker laten verwerken als de Verantwoordelijke wel bezwaar heeft gemaakt.
- 5.6 Wanneer Verwerkingsverantwoordelijke bezwaar heeft, zal Verwerker in redelijkheid naar een oplossing zoeken om te voorkomen dat Verwerkingsverantwoordelijke het Contract tussentijds moet beëindigen. Indien Verwerkingsverantwoordelijke zich genoodzaakt voelt om het Contract te beëindigen zal dit kosteloos zijn.
- 5.7 Alleen in bedrijfskritische omstandigheden zoals de noodzaak om acuut aanvullende security-maatregelen te treffen, mag Verwerker afwijken van deze procedure. Verwerker zal Verantwoordelijke altijd zo snel mogelijk informeren over de nieuwe sub-verwerker, met onderbouwing van de noodzaak om deze Verwerker acuut in te schakelen. Verwerker zal de Verwerkingsverantwoordelijke alsnog in de gelegenheid stellen om bezwaar te maken.

6. Verlenen bijstand in verband met gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging en informatieplicht

- 6.1 De Verwerker stelt de voor de Verwerkingsverantwoordelijke alle informatie ter beschikking die nodig is om aan te tonen dat de in deze bepalingen neergelegde verplichtingen worden nageleefd en rechtstreeks voortvloeien uit Algemene Verordening Gegevensbescherming en/of relevante

privacy wetgeving. Op verzoek van de Verwerkingsverantwoordelijke staat de Verwerker ook audits toe van en werkt hij mee aan de verwerkingsactiviteiten die onder deze bepalingen vallen, met redelijke tussenpozen of indien er aanwijzingen van niet-naleving zijn. Verwerkingsverantwoordelijke zal hierbij rekening houden met relevante certificeringen waarover de Verwerker al beschikt.

- 6.2 De Verwerkingsverantwoordelijke kan ervoor kiezen de audit zelf uit te voeren of een onafhankelijke auditor inschakelen. Audits kunnen ook inspecties in de gebouwen of fysieke faciliteiten van de Verwerker betreffen en worden met inachtneming van een redelijke termijn uitgevoerd.
- 6.3 Verwerker verleent desgevraagd kosteloos bijstand aan Verantwoordelijke indien met betrekking tot de verwerking een beoordeling wordt gemaakt van het effect van de verwerkingsactiviteiten op de bescherming van Persoonsgegevens (gegevensbeschermingseffectbeoordeling). Dit betekent onder meer medewerking aan het desgewenst verlenen van inzage in logs en overeenkomsten met sub-verwerkers, maar strekt zich niet uit tot het verlenen van juridische ondersteuning bij het opstellen van een dergelijk rapport.
- 6.4 Verwerker verleent desgevraagd bijstand aan Verantwoordelijke indien naar aanleiding van een gegevensbeschermingseffectbeoordeling door Verantwoordelijke raadpleging van de Autoriteit Persoonsgegevens plaatsvindt.
- 6.5 Indien uit een (voorafgaand of ambtshalve) onderzoek van de Autoriteit Persoonsgegevens of uit jurisprudentie zou blijken dat Verwerker, of haar sub-verwerkers, (op onderdelen) niet aan de Algemene Verordening Gegevensbescherming en/of andere relevante privacywetgeving voldoet, zal Verwerker Verantwoordelijke hierover onverwijld informeren. Verwerker zal alle benodigde technische of organisatorische verbeteringen die hieruit voortvloeien, op eigen kosten doorvoeren.

7. Beveiligen Persoonsgegevens

- 7.1 Verwerker zorgt ervoor dat de Persoonsgegevens voldoende worden beveiligd. Om verlies en onrechtmatige verwerkingen te voorkomen neemt Verwerker passende technische en organisatorische maatregelen.
- 7.2 Deze maatregelen zijn afgestemd op het risico van de Verwerking. Een overzicht van deze maatregelen en het beleid daaromtrent wordt opgenomen in Annex 2.
- 7.3 Ter controle van de genomen beveiligingsmaatregelen zal Verwerker aan Verwerkingsverantwoordelijke op eerste verzoek, met een maximum van een keer per jaar, een rapportage sturen waarin de genomen actuele beveiligingsmaatregelen staan en de eventuele aandachts- en/of verbeterpunten. Hiervoor brengt Verwerker geen kosten in rekening aan Verwerkingsverantwoordelijke.
- 7.4 Verwerkingsverantwoordelijke mag een audit laten uitvoeren om te bepalen of het verwerken van de Persoonsgegevens aan de wet en de afspraken uit deze Verwerkersovereenkomst voldoet. Verwerker verleent hierbij zijn medewerking. Waaronder het toegang verlenen tot gebouwen en databases en het ter beschikking stellen van alle relevante informatie.
- 7.5 De kosten voor de uitvoering van deze audit zullen voor rekening van Verwerker komen wanneer blijkt dat Verwerker zich niet aan de verplichtingen in deze Verwerkersovereenkomst houdt.

- 7.6 De controle op de algehele verwerking van Persoonsgegevens door Verwerker kan, naast de auditmogelijkheid, ook geschieden via zelfevaluatie door Verwerker. Verwerker zal hierbij aan Verwerkingsverantwoordelijke een rapport verstrekken waarin Verwerker aantoont dat hij voldoet aan de wet en de afspraken uit deze Verwerkersovereenkomst. Deze rapportage dient te worden ondertekend door een directielid binnen de organisatie van Verwerker.
- 7.7 Wanneer Partijen vinden dat een wijziging in de te nemen beveiligingsmaatregelen noodzakelijk is, treden Partijen in overleg over de wijziging daarvan. De kosten gemoeid met het wijzigen van de beveiligingsmaatregelen komen voor rekening van degene die de kosten maakt.

8. Geheimhouding

- 8.1 Verwerker zal de verstrekte Persoonsgegevens geheim houden, tenzij dit op basis van een wettelijke verplichting niet kan.
- 8.2 Verwerker zorgt dat zijn/haar personeel en ingeschakelde hulppersonen zich aan deze geheimhouding houden, door bijvoorbeeld een geheimhoudingsplicht in de (arbeids-) contracten op te nemen.

9. Datalekken

- 9.1 In geval van een ontdekking van een mogelijk Datalek zal Verwerker Verwerkingsverantwoordelijke hierover zo spoedig mogelijk informeren, maar in ieder geval binnen een termijn van 24 uur, overeenkomstig het proces uit Annex 3 zodat Verwerkingsverantwoordelijke indien nodig een melding van het Datalek bij de Toezichthouder kan doen.
- 9.2 Verwerker zal Verwerkingsverantwoordelijke op de hoogte houden van nieuwe ontwikkelingen rondom het Datalek. Ook zal Verwerker onmiddellijk alle maatregelen treffen die redelijkerwijs noodzakelijk zijn om het Datalek te beëindigen dan wel te beperken om een soortgelijk incident in de toekomst te (kunnen) voorkomen.
- 9.3 Verwerker mag geen melding van een Datalek aan de Toezichthouder doen, wanneer bij het Datalek Persoonsgegevens van Verwerkingsverantwoordelijke betrokken zijn. Ook mag Verwerker de Betrokkenen niet informeren over het Datalek. Verantwoordelijke beoordeelt of de Toezichthouder en/of Betrokkene wordt geïnformeerd. Indien de wetgeving dit vereist zal Opdrachtnemer meewerken aan het informeren van de ter zake relevante autoriteiten en/of betrokkenen.
- 9.4 Eventuele kosten die gemaakt worden om het Datalek op te lossen en in de toekomst te kunnen voorkomen, komen voor rekening van degene die de kosten maakt.

10. Aansprakelijkheid

- 10.1 Als Verwerker de verplichtingen uit deze Verwerkersovereenkomst niet nakomt, kan Verwerkingsverantwoordelijke Verwerker daarvoor aansprakelijk stellen.

10.2 Verwerker is aansprakelijk voor alle schade die Verwerkingsverantwoordelijke lijdt door het niet nakomen van de wet en de bepalingen uit deze Verwerkersovereenkomst, voor zover dit is ontstaan door toedoen of nalaten van Verwerker.

10.3 Indien Verwerker de verplichtingen in deze Verwerkersovereenkomst overtreedt, is Verwerker aan Verwerkingsverantwoordelijke een direct opeisbare boete verschuldigd van €15.000 en €500 voor iedere dag dat Verwerker de overtreding laat voortduren. Daarnaast behoudt Verwerkingsverantwoordelijke het recht om schadevergoeding te vorderen.

10.4 Verwerker vrijwaart Verantwoordelijke van eventuele aanspraken van derde partijen, waaronder uitdrukkelijk begrepen toezichthouders zoals de Autoriteit Persoonsgegevens en Betrokkenen, gebaseerd op of voortvloeiend uit een schending van de Algemene Verordening Gegevensbescherming en/of dit Contract die aan de Verwerker kan worden toegerekend.

11. Teruggave Persoonsgegevens en bewaartermijn

11.1 Na het beëindigen van deze Verwerkersovereenkomst zal Verwerker de Persoonsgegevens ter beschikking stellen in gangbaar digitaal formaat aan Verwerkingsverantwoordelijke.

11.2 Zonder andersluidende schriftelijke instructie van Verwerkingsverantwoordelijke, zal Verwerker (kopieën van) de Persoonsgegevens 30 dagen na beëindiging van deze Verwerkersovereenkomst vernietigen. Voor de back-ups geldt een maximum vernietigingsperiode van 30 dagen.

11.3 Verwerker zal na de teruggave en/of vernietiging van de Persoonsgegevens schriftelijk aan Verwerkingsverantwoordelijke verklaren niet langer in het bezit te zijn van de Persoonsgegevens.

12. Toepasselijk recht en geschillenbeslechting

12.1 De Verwerkersovereenkomst en de uitvoering daarvan worden beheerst door het Nederlands recht.

12.2 Eventuele geschillen die tussen Partijen ontstaan, verband houdende met deze Verwerkersovereenkomst, worden voorgelegd aan de bevoegde rechter in Nederland.

13. Slotbepalingen

13.1 Deze Verwerkersovereenkomst is onderdeel van het Contract. Alle rechten en verplichtingen uit het Contract zijn daarom ook van toepassing op de Verwerkersovereenkomst.

13.2 Bij eventuele tegenstrijdigheden tussen de bepalingen in de Verwerkersovereenkomst en het Contract, gelden de bepalingen uit deze Verwerkersovereenkomst ten aanzien van de verwerking van Persoonsgegevens.

13.3 Afwijkingen van deze Verwerkersovereenkomst zijn slechts geldig wanneer Partijen dit samen schriftelijk zijn overeengekomen.

Aldus door Partijen overeengekomen en ondertekend:

Verwerkingsverantwoordelijke:

Ondertekend voor en namens Stichting het Juridisch Loket

Naam: [...]

Functie:

Datum en plaats:

Handtekening:

Verwerker:

Ondertekend voor en namens [STATUTAIRE NAAM]

Naam:

Functie:

Datum en plaats:

Handtekening:

Annex 1: Overzicht met verwerkingen van Persoonsgegevens en verwerkingsdoelen

Het onderstaande schema zal samen met de verwerker 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.

Algemene beschrijving verwerkingsactiviteiten door Verwerker:	
--	--

Verwerkingsdoelen:	Beschrijving per doeleinde
1.	
2.	
3.	

Sub-verwerkers per verwerkingsdoeleinde:	Naam	Adres	Vestiging/locatie
1.			
2.			
3.			

Verwerkte (categorieën van) persoonsgegevens per doeleinde:	
1.	
2.	
3.	

Bewaartermijnen per verwerkingsdoeleinde / persoonsgegevens:	
1.	
2.	
3.	

Annex 2: Overzicht met beveiligingsmaatregelen

Deze annex dient te worden ingevuld door de Verwerker

Deel 1: Informatiebeveiligingsnorm

De Verwerker hanteert de volgende informatiebeveiligingsnorm (kruis aan wat van toepassing is):

- ☐ ISO 27001
- ☐ ISAE 3402
- ☐ Anders, namelijk _____
- ☐ Geen norm (verplicht Deel 2 invullen)

De Verwerker toont aan dat het niveau van informatiebeveiliging toereikend is. De toereikendheid blijkt uit (doorhalen wat niet van toepassing is):

- ☐ Certificering / derden verklaring

Naam certificaat	Organisatieonderdeel/ dienst waarop het certificaat betrekking heeft	Geldigheidsduur certificaat	Verklaring van toepasselijkheid
			Indien aanwezig dient de Verwerker deze mee te sturen

- ☐ Anders, namelijk _____
- ☐ Geen aantoonbare toereikendheid (mogelijk Deel 2 alsnog verplicht).

Deel 2: Organisatorische en technische beveiligingsmaatregelen

Indien Deel 1 niet van toepassing is, dient Deel 2 ingevuld te worden door Verwerker om aan te tonen dat passende technische en organisatorische maatregelen zijn getroffen.

De Verwerker heeft tenminste onderstaande beveiligingsmaatregelen getroffen (kruis aan wat van toepassing is):

Onderwerp	Maatregel	Aanwezig	Niet aanwezig	Niet van toepassing

Beleid	Informatiebe- veiligingsbeleid*			
Veilig personeel	VOG			
	Awareness en training van personeel			
	Geheimhoudingsverklaring voor (ingehuurde) medewerkers			
Toegangsbeleid	Fysiek toegangsbeleid			
	Autorisatiebeleid			
	Wachtwoord-beleid			
	Twee factor authenticatie			
	Logging- en monitorings beleid**			
Incident- management	Procedure beveiligingsinci- denten en datalekken			
Continuïteit	Back-up en restore beleid			
	Business continuity plan			
Bedrijfsmiddelen	Beleid veilig gebruik maken van bedrijfsmiddelen en systemen			
Cryptografie (versleuteling)	Encryptie in transit			
	Encryptie at rest			
Informatie- systemen	Beleid aanschaf, ontwikkeling en onderhoud van informatie-systemen			
Onafhankelijke beoordelingen	Interne audit			
	Externe audit			
	Penetratie test			
	Vulnerability check			
Anders, nl.				

* Graag toelichten of het informatiebeveiligingsbeleid regels bevat over naleving van de NCSC richtlijnen voor webapplicaties en top 10 OWASP kwetsbaarheden.

** Graag de procedure toelichten voor systematische en incidentele controle van de logs

Annex 3: Proces rondom het melden van Datalekken en de te verstrekken informatie

Wat is een beveiligingsincident en datalek?

Een Datalek is een beveiligingsincident waarbij Persoonsgegevens, die de Verwerker namens de Verwerkingsverantwoordelijke beheert, mogelijk verloren zijn gegaan of onbedoeld toegankelijk waren voor derden. Het gaat om gegevens die te koppelen zijn aan deze personen, zoals, maar niet beperkt tot, namen, adressen, telefoonnummers, e-mailadressen, login-gegevens, cookies, IP-adressen of identificerende gegevens van computers of telefoons.

Ter illustratie je een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld:

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

Waar moet gemeld worden?

Telefoon: 0118-652013

Of

E-mail: privacyofficer@juridischloket.nl

Wat moet gemeld worden? Geef antwoord op de onderstaande vragen.

1. Geef een samenvatting van het 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 van de groep personen om wiens gegevens het gaat.

Geef aan of het gaat om medewerkersgegevens of gegevens van klanten. Bijzondere aandacht verdienen gegevens van een kwetsbare groepen personen, zoals sociaal economische hulpbehoevende, minderjarige, etc.
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?

Heb je (al) 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, mogelijke begin- en eindtijd.

8. De naam en de contactgegevens van de functionaris voor gegevensbescherming, Privacy Officer of een ander contactpersoon waar meer informatie kan worden verkregen.

9. De waarschijnlijke gevolgen voor de personen wiens persoonsgegevens zijn gelekt;

10. De maatregelen die worden voorgesteld of zijn genomen om de inbreuk in verband met persoonsgegevens aan te pakken ter beperking van de eventuele nadelige gevolgen.

Verwerker garandeert dat de door hem verstrekte informatie volledig, correct en actueel is. De meldplicht van Verwerker aan Verantwoordelijk zoals hierboven beschreven geldt ongeacht de impact van de inbreuk.