Verwerkersovereenkomst GGDrU

Mobiliteitskaarten

Tussen

<Partij>

en

GGD Regio Utrecht

Inhoudsopgave

1. DEFINITIES 2
2. TOTSTANDKOMING, DUUR, BEËINDIGING EN HERLEVEN 2
3. VERWERKEN PERSOONSGEGEVENS 3
4. BEVEILIGEN VAN PERSOONSGEGEVENS 3
5. VERWERKING BUITEN DE EU 4
6. INSCHAKELEN VAN SUB-VERWERKERS 4
7. GEHEIMHOUDING 4
8. DATALEKKEN 5
9. RECHTEN VAN DE BETROKKENE 5
10. AANSPRAKELIJKHEID 5
11. TERUGGAVE PERSOONSGEGEVENS EN BEWAARTERMIJN 6
12. SLOTBEPALINGEN 6

BIJLAGE 1: OVERZICHT VERWERKINGEN 8
BIJLAGE 2: OVERZICHT BEVEILIGINGSMAATREGELEN 10
BIJLAGE 3: PROCES DATALEKKEN 11

GGD regio Utrecht

De GGD Regio Utrecht hecht veel waarde aan de privacy van de betrokkenen en een veilige verwerking van gegevens. Deze overeenkomst helpt partijen om samen te voldoen aan de AVG-wetgeving, zodat beiden professioneel en vertrouwd kunnen samenwerken.

Contractspartijen:

1. <bedrijf, afdeling>, gevestigd te <adres>, ingeschreven in het handelsregister onder KvK nummer <KvK nummer>, rechtsgeldig vertegenwoordigd door <persoonsnaam>, <functie>, hierna te noemen: "**Verwerker**";

en

2. GGD regio Utrecht, gevestigd en kantoorhoudende aan De Dreef 5, 3706 BR te Zeist, ingeschreven in het handelsregister onder KvK nummer 50909185, vertegenwoordigd door de Directeur publieke gezondheid van GGD regio Utrecht, dr. M. Sprenger, als verwerkingsverantwoordelijke, hierna te noemen: "**Verantwoordelijke**".

Individueel aan te duiden als "**Partij**" en gezamenlijk als "**Partijen**".

Overwegende dat:

A. Partijen hebben op [datum] een of meerdere (deel)overeenkomst(en) met betrekking tot [***] gesloten (hierna de: "**Hoofdovereenkomst**"). Ter uitvoering van de Hoofdovereenkomst worden persoonsgegevens verwerkt.

B. Partijen leggen in deze overeenkomst en de integraal daarbij behorende bijlagen (hierna de "**Verwerkersovereenkomst**") de rechten en plichten over en weer vast met betrekking tot de verwerking van persoonsgegevens.

Komen overeen:

1. Definities

1.1 De begrippen uit deze Verwerkersovereenkomst hebben dezelfde betekenis als de begrippen uit de AVG en de UAVG, tenzij expliciet anders aangegeven.

1.2 In deze overeenkomst wordt verstaan onder verwerken van persoonsgegevens, op basis van de definitie van artikel 4 AVG, het verwerken daarvan door Verwerker in opdracht van Verantwoordelijke, waaronder begrepen persoonsgegevens die door Verantwoordelijke aan Verwerker zijn verstrekt of die door Verwerker namens Verantwoordelijke worden verzameld of opslaat in het kader van het uitvoeren van deze overeenkomst en/of de Hoofdovereenkomst.

2. Totstandkoming, duur, beëindiging en herleven

2.1 Aanvang: Deze Verwerkersovereenkomst gaat in bij ondertekening of op het eerdere moment dat de feitelijke verwerking namens Verantwoordelijke is gestart. De overeenkomst geldt niet voor verwerkingen waarvoor Verwerker zelfstandig verwerkingsverantwoordelijke is.

2.2 Duur: Deze Verwerkersovereenkomst is onderdeel van de Hoofdovereenkomst en zal gelden voor de duur daarvan en zoveel langer als Verwerker persoonsgegevens verwerkt. Als de Hoofdovereenkomst eindigt, eindigt deze Verwerkersovereenkomst automatisch volgens de hierin overeengekomen bepalingen.

2.3 Wijzigingen: Anders dan met schriftelijke instemming van Partijen, kan deze Verwerkersovereenkomst gedurende de looptijd niet worden opgezegd, vernietigd,

of anderszins worden gewijzigd of beëindigd, tenzij wijzigingen in toepasselijke regelgeving aanpassing van deze overeenkomst noodzakelijk maken. De Verwerkersovereenkomst kan niet apart van de Hoofdovereenkomst worden opgezegd.

2.4 Herleven: Indien onverhoopt na definitief beëindigen van de Verwerkersovereenkomst, alsnog persoonsgegevens waarop deze overeenkomst van toepassing was, worden verwerkt door Verwerker of diens sub-verwerkers, herleven alle bepalingen van de Verwerkersovereenkomst.

3. Verwerken persoonsgegevens

3.1 Verantwoordelijke behoudt de volledige zeggenschap over het doel van en de essentiële middelen voor de verwerking van de persoonsgegevens.

3.2 Verwerker heeft geen zeggenschap over de persoonsgegevens en neemt geen besluiten over het gebruik, de verstrekking aan derden of de bewaartermijn, tenzij Verantwoordelijke daar vooraf schriftelijk opdracht toe geeft.

3.3 Verwerker verwerkt de persoonsgegevens op zorgvuldige wijze, uitsluitend volgens de instructies van Verantwoordelijke en conform de bepalingen van deze overeenkomst en de AVG.

3.4 Verwerker verleent tijdig en redelijk de noodzakelijke bijstand aan Verantwoordelijke bij de nakoming van wettelijke verplichtingen, waaronder het uitvoeren van een DPIA en het afhandelen van rechten van betrokkenen, voor zover dit redelijkerwijs van Verwerker mag worden verwacht. Verwerker kan voor een DPIA-bijstand een redelijke vergoeding vragen, tenzij de bijstand noodzakelijk is door een fout van Verwerker of reeds verdisconteerd in de Hoofdovereenkomst.

3.5 Verwerker verwerkt de persoonsgegevens uitsluitend voor zover en zolang dit noodzakelijk is voor de uitvoering van de Hoofdovereenkomst met inachtneming van het bepaalde in de Verwerkersovereenkomst.

4. Beveiligen van Persoonsgegevens

4.1 Verwerker treft passende technische en organisatorische maatregelen conform artikel 32 AVG. Deze maatregelen zijn afgestemd op het verwerkingsrisico en de stand van de techniek. De minimale maatregelen zijn vastgelegd in Bijlage 2.

4.2 Indien de verwerking betrekking heeft op bijzondere persoonsgegevens (zoals bedoeld in art. 9 AVG), garandeert Verwerker een verhoogd beveiligingsniveau dat aansluit bij de gevoeligheid van deze gegevens.

4.3 Verwerker verstrekt op verzoek jaarlijks kosteloos een rapportage over de effectiviteit van de beveiligingsmaatregelen en eventuele verbeterpunten en termijnen van oplossen daarvan. Indien Verwerker bijzondere gegevens verwerkt, wordt deze rapportage automatisch jaarlijks verstrekt.

4.4 Verantwoordelijke heeft het recht om door zelf of door een onafhankelijke auditor een audit te laten uitvoeren naar de naleving van deze overeenkomst en de AVG. Verwerker verleent hiertoe tijdig alle redelijke medewerking, inclusief toegang tot relevante locaties, gegevensdragers en informatie.

4.5 Verantwoordelijke maakt bij voorkeur eerst gebruik van de rapportages en zelfevaluaties. Een audit op locatie vindt alleen plaats indien er een gegronde reden is of indien de verstrekte rapportages onvoldoende uitsluitsel geven.

4.6 Partijen treden vooraf in overleg over de omvang en planning van de audit om de operationele verstoring tot een minimum te beperken.

4.7 De kosten van de audit worden gedragen door Verantwoordelijke, tenzij de audit aantoont dat Verwerker tekort is geschoten in de nakoming van deze overeenkomst; in dat geval draagt Verwerker de kosten.

4.8 Aanvullend op het auditrecht verstrekt Verwerker op verzoek een door de directie ondertekend zelfevaluatierapport, waarin wordt aangetoond hoe Verwerker aan de wettelijke en contractuele afspraken voldoet.

4.9 Indien wijziging van de beveiligingsmaatregelen noodzakelijk is, treden Partijen in overleg. Redelijke kosten voor wijzigingen voortvloeiend uit gewijzigde wetgeving of tekortkomingen van Verwerker komen voor rekening van Verwerker.

5. Verwerking buiten de EU

5.1 Verwerker verwerkt geen persoonsgegevens buiten de Europese Unie (EU) zonder voorafgaande schriftelijke toestemming van Verantwoordelijke. Deze toestemming wordt in beginsel niet verleend, tenzij uitdrukkelijk anders overeengekomen en uitsluitend als:

a) de Europese Commissie voor het betreffende land een adequaatheidsbesluit heeft genomen (art. 45 AVG); of
b) de verwerking geschiedt op basis van goedgekeurde bindende bedrijfsvoorschriften (art. 47 AVG).

5.2 Indien Verwerker een verwerking buiten de EU voorziet, meldt hij dit onverwijld en schriftelijk aan Verantwoordelijke. Verantwoordelijke kan in dat geval aanvullende eisen stellen of de voorgenomen verwerking weigeren toe te staan. Indien partijen geen overeenstemming bereiken over de verwerking buiten de EU, heeft Verantwoordelijke het recht de Hoofdovereenkomst (voor het betreffende deel) kosteloos en per direct te beëindigen.

5.3 Toestemming wordt geacht te zijn verleend voor de sub-verwerkers die bij het aangaan van deze overeenkomst reeds schriftelijk zijn gemeld en die voldoen aan de voorwaarden in 5.1 sub a en b.

6. Inschakelen van sub-verwerkers

6.1 Het is Verwerker toegestaan conform 28 lid 2 AVG sub-verwerkers en de bepalingen van deze overeenkomst in te schakelen en/of te wisselen, mits Verantwoordelijke daarover vooraf is geïnformeerd en de mogelijkheid is geboden om met redenen omkleed bezwaar te maken.

6.2 Het is Verwerker niet toegestaan om, zonder schriftelijke toestemming van Verantwoordelijke een sub-verwerker in te schakelen of te wisselen wanneer die sub-verwerker bijzondere persoonsgegevens verwerkt.

6.3 Indien Verantwoordelijke toestemming geeft voor het inschakelen van Sub-verwerker(s), dan sluit Verwerker een schriftelijke overeenkomst met de Sub-verwerker(s) af, waarbij aan de sub-verwerker(s) minstens dezelfde verplichtingen worden opgelegd als aan Verwerker in het kader van deze Verwerkersovereenkomst.

6.4 Verwerker is jegens Verantwoordelijke aansprakelijk voor de fouten van sub-verwerkers op dezelfde wijze als voor eigen fouten, met inachtneming van de aansprakelijkheidsregeling in de Hoofdovereenkomst.

7. Geheimhouding

7.1 Verwerker houdt de aan hem verstrekte persoonsgegevens strikt geheim, tenzij dit op basis van een wettelijke verplichting niet mogelijk is. In dat geval stelt de Verwerker Verantwoordelijke in kennis van de beoogde verwerking en het wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

7.2 Toegang tot de persoonsgegevens is beperkt tot personen voor wie dit noodzakelijk is voor de uitvoering van de Hoofdovereenkomst.

7.3 Verwerker waarborgt dat de persoonsgegevens geheim blijven, dat alle personen met toegang schriftelijk tot geheimhouding zijn gebonden en dat deze personen de geheimhoudingsverplichting strikt naleven.

8. Datalekken

8.1 Om Verantwoordelijke in staat te stellen correct aan haar AVG verplichtingen te voldoen, zal Verwerker direct na ontdekking van een (mogelijk) datalek, doch uiterlijk binnen 24 uur, Verantwoordelijke informeren conform Bijlage 3.

8.2 Na iedere melding van een datalek houdt de Verwerker de Verantwoordelijke proactief op de hoogte van nieuwe ontwikkelingen, de genomen herstelmaatregelen en de stappen om herhaling te voorkomen.

8.3 Het is de Verwerker niet toegestaan het datalek te melden bij de Toezichthouder of betrokkene(n), tenzij de Verantwoordelijke hiervoor uitdrukkelijk opdracht geeft. Verantwoordelijke kan kiezen om bij meldingen aan toezichthouder(s) ook Verwerker daarover te informeren.

8.4 De bijlage beschrijft het overeengekomen proces bij datalekken en de te verstrekken informatie. Om het incident te kunnen beoordelen verschaft Verwerker alle inlichtingen aan Verantwoordelijke die hij zelf redelijkerwijs van belang acht en alle informatie die Verantwoordelijke redelijkerwijs additioneel noodzakelijk acht.

8.5 Iedere Partij draagt de eigen kosten voor het oplossen en in de toekomst voorkomen van datalekken, onverminderd het recht van Verantwoordelijke om deze kosten als schade te verhalen indien het datalek toerekenbaar is aan Verwerker.

9. Rechten van de Betrokkene

9.1 De Verwerker verleent passende medewerking aan de uitvoering van de rechten van betrokkenen (art. 12-22 AVG).

9.2 Indien de Verwerker rechtstreeks een verzoek van een betrokkene ontvangt, wordt dit direct, doch uiterlijk binnen 2 werkdagen, schriftelijk doorgeleid naar de Verantwoordelijke en handelt Verwerker dit verzoek niet zelf af.

9.3 Medewerking door Verwerker wordt zodanig verleend dat Verantwoordelijke op hem rustende wettelijke termijnen kan halen.

10. Aansprakelijkheid

10.1 De Verwerker is uitsluitend aansprakelijk voor schade door een toerekenbare tekortkoming in de nakoming van deze overeenkomst of een aan hem toe te rekenen inbreuk op de AVG. Vergoeding van deze schade door de Verwerker is niet afhankelijk van voorwaarden uit een door hem gesloten verzekering.

10.2 Onder schade wordt mede verstaan vermogens- en immateriële schade en schade in de zin van art. 82 AVG.

10.3 Partijen komen onderling overeen dat aan betrokkene(n) verschuldigde schadevergoedingen en bestuurlijke boetes als schade van Verantwoordelijke worden aangemerkt, mits deze rechtstreeks voortvloeien uit een aan Verwerker toerekenbare tekortkoming of overtreding.

10.4 De omvang van de aansprakelijkheid is beperkt tot schade die, gelet op de aard en de ernst van de tekortkoming, in redelijke verhouding staat tot het handelen of nalaten van Verwerker. Het niet behalen van wettelijke termijnen voor datalekken en de niet (tijdige) afhandeling van meldingen van betrokkenen geldt, behoudens overmacht, altijd als een ernstige tekortkoming.

10.5 Voor zover Partijen een aansprakelijkheidslimiet zijn overeengekomen in de Hoofdovereenkomst of Bijlage 1, geldt deze limiet, tenzij er sprake is van opzet of bewuste roekeloosheid. Een limiet wordt in de regel niet geaccepteerd wanneer Verwerker bijzondere persoonsgegevens verwerkt. Bij verwerking van gevoelige gegevens wordt de gemaakte afweging over de limiet expliciet in deze overeenkomst toegelicht.

10.6 De omvang van de schade, en daarmee de hoogte van de schadevergoeding, wordt vastgesteld zodra deze volledig in kaart is gebracht. Zolang de schade voortduurt, behoudt de Verantwoordelijke zich het recht voor de omvang tussentijds vast te stellen met onderbouwde schattingen.

10.7 De Verantwoordelijke dient de Verwerker zo spoedig mogelijk te informeren over eventuele schade.

11. Teruggave Persoonsgegevens en bewaartermijn

11.1 Na het beëindigen van deze Verwerkersovereenkomst geeft Verwerker de Persoonsgegevens terug, in een voor de Verantwoordelijke gangbaar, gestructureerd en machine leesbaar formaat, tenzij Verantwoordelijke tegen die tijd anders bepaalt. Eventuele achter gebleven persoonsgegevens zullen op een zorgvuldige en veilige manier worden vernietigd en Verwerker verstrekt daartoe een schriftelijk verklaring.

11.2 Indien nodig stelt Verwerker op verzoek een exit-plan op voor een soepele overdracht naar een opvolgende partij. Deze medewerking geschiedt tegen de reguliere tarieven, tenzij de beëindiging voortvloeit uit een toerekenbare tekortkoming van Verwerker. Vernietiging van gegevens vindt te allen tijde kosteloos plaats.

11.3 De persoonsgegevens die Verwerker verwerkt volgens deze Verwerkersovereenkomst zullen worden vernietigd na verstrijken van de overeengekomen bewaartermijn(en) en/of terstond op verzoek van Verantwoordelijke.

12. Slotbepalingen

12.1 Deze Verwerkersovereenkomst vormt een integraal onderdeel van de Hoofdovereenkomst. Alle rechten en verplichtingen uit de Hoofdovereenkomst zijn onverkort van toepassing, tenzij deze overeenkomst daar expliciet van afwijkt.

12.2 Voor zover wettelijk toegestaan meldt Verwerker relevante wijzigingen in zijn (indirecte) zeggenschap of eigendomsstructuur onverwijld aan Verantwoordelijke. Indien hierdoor de bescherming van persoonsgegevens in het geding komt, treden Partijen in overleg. Indien geen passende waarborgen kunnen worden geboden, mag Verantwoordelijke de (Hoofd)overeenkomst(en) zonder schadeverplichting beëindigen.

12.3 Indien de voortzetting van deze overeenkomst, door omstandigheden toerekenbaar aan of direct gerelateerd aan Verwerker, het maatschappelijk vertrouwen in de publieke taak van Verantwoordelijke ernstig schaadt, is Verantwoordelijke gerechtigd de overeenkomst met een redelijke opzegtermijn te beëindigen. Verwerker verleent alsdan volledige medewerking aan de exit-procedure (artikel 11.2) tegen de dan geldende reguliere tarieven.

12.4 Bij tegenstrijdigheid tussen de Hoofdovereenkomst en deze Verwerkersovereenkomst prevaleren de bepalingen van deze Verwerkersovereenkomst voor zover het de verwerking van persoonsgegevens betreft. Aanvullingen of afwijkingen zijn alleen geldig indien deze schriftelijk door beide Partijen zijn overeengekomen.

12.5 Op deze verwerkersovereenkomst is Nederlands recht van toepassing. Geschillen die niet in der minne kunnen worden geschikt, worden uitsluitend voorgelegd aan de bevoegde rechter in het arrondissement waar Verantwoordelijke gevestigd is.

Aldus door Partijen overeengekomen en ondertekend:

De Verwerker

Ondertekend voor en namens :

Naam :

Functie : <kvk check op bevoegdheden?>

Datum en plaats :

Handtekening :

De Verantwoordelijke

Ondertekend voor en namens :

Naam :

Functie : <Alleen DT bevoegd te tekenen, tenzij ondertekenaar schriftelijk gevolmachtigd of mandaat>

Datum en plaats :

Handtekening :

Bijlage 1: Overzicht Verwerkingen

Overzicht met verwerkingen van Persoonsgegevens en verwerkingsdoelen

Naam verwerkingsactiviteit:	*Tip – gebruik een naam die aansluit bij de feitelijke praktijk bij de GGD (Bijv. "Salarisadministratie", "Coronavaccinatie" of "Inkoop IT-middelen")*
Verwerkingsactiviteiten, (proces) beschrijving van activiteiten door Verantwoordelijke:	*Wat doet de GGD met de persoonsgegevens, wat is de handelingen die worden gedaan met de gegevens? Nb process*
Verwerkingsdoelen:	*De GGD verwerkt de voornoemde gegevens met een doel, welk doel is dat? (Uitvoeren aan publieke taak, welke? Artikel(en) van welke wet?)*
Beschrijving rol verwerker voornoemde verwerkingsactiviteiten:	*Wat besteedt de GGD precies uit aan deze partij? (Bijv. "Deze partij levert alleen de software waarin wij werken" of "Deze partij voert de data-analyse voor ons uit"). Wat doet de verwerker in voornoemde activiteit wel voor de GGD, wat doet de verwerker niet? De instructie mogen ook in de Hoofdovereenkomst zijn afgebakend, dan een verwijzing daarnaar.*
Categorie(ën) van betrokkenen bij deze activiteit van de GGD:	*Noem alle categorieën die van toepassing zijn. Bijv. Patiënten, cliënten, inwoners regio X, werknemers, klanten, kinderen, kwetsbare mensen (oggz), aan infectie ziekte blootgestelde, etc.*
Soorten persoonsgegevens die door Verwerker zullen worden verwerkt:	*Benoem elke soort als die wordt verwerkt, bijvoorbeeld: Normale gegevens: NAW, mail, telefoon, geboortedatum, cliëntnummer, dossiernummer, planning afspraken, IP-adres en gebruikers log. Gevoelige gegevens: sociaal maatschappelijke gegevens, leefomstandigheden, zorgbegeleiding, financieel administratief, werk HR verzuim en BIG registratie, gegevens over kinderen, BSN. Bijzondere gegevens: alle gezondheidsgegevens over een persoon, medisch dossier, behandelgegevens, gegevens lichamelijke of mentale gezondheid, vaccinaties, diagnoses, jeugd of gezinssituatie voor gezondheid relevant.*
In geval van gezondheidsgegevens (NEN-7510):	*Hoe heeft Verwerker beveiligingsmaatregelen ingericht gelijkwaardig aan NEN-7510 voor de verwerkingsactiviteiten?*
Contactpersoon Verantwoordelijke:	*1. Contract/functioneel eigenaar GGD intern* 2. privacyofficer@ggdru.nl Tel 030-6086086
Contactpersoon Verwerker:	*Contact persoon regulier* *Contact persoon bij escalatie* *Contactpersoon datalekken*
Locatie(s) verwerkingen:	*Land of regio, Cloud of fysieke opslag, onderscheid tussen productie en back-up?*
Verwerking buiten de EU/EER:	*Voldoet de verwerking aan een van de uitzonderingen in art. 5 van deze Verwerkersovereenkomst?*

Toegestane Sub-verwerker(s): • Rol: • KvK-nummer: • Locatie data (server) • Verwerkersovereenomst met Verwerker? (ja/nee) • Verwerker bevestigd dat beveiligingsmaatregelen conform eisen zijn?	*Alle sub-verwerkers die verwerken benoemen.* *NB, met benoemen is toestemming mits goedgekeurd geregeld.* *Rol: globale beschrijving van activiteiten die ze voor Verwerker verrichten, en of en zo ja welke categorieën van persoonsgegevens ze verwerken.*
Bewaartermijn:	*Concrete termijn of trigger? Afgeleid van wettelijke plicht, zo ja welke, of bewaartermijn afhankelijk van instructies?*
Afspraken verwijderen na einde dienstverlening of verloop bewaartermijn:	*Wat is de afspraak bij het einde van de Hoofdovereenkomst? Verwijderen, overdragen, retourneren?* *Zijn er voorwaarden aan de wijze van vernietigen (manier waarop, bewijs daarvan) of vorm van overdragen?*
Aansprakelijkheidslimiet volgens art. 10.5	*bijv. de jaarwaarde van de opdracht of een specifiek bedrag*

Bijlage 2: Overzicht beveiligingsmaatregelen

Hier moet een overzicht van de beveiligingsnormen opgenomen worden die Verwerker hanteert. Status en dekking. Als er geen normen worden gebruikt of als de verwerker niet is gecertificeerd op de normen, beschrijft de Verwerker de relevante maatregelen die zijn genomen op het gebied van informatiebeveiliging.

Louter in het geval dat Verwerker bijzondere persoonsgegevens (Gezondheidsgegevens) zal verwerken, is het van belang te toetsen of er aan beveiligingsmaatregelen NEN-7510 wordt voldaan. Over ieder hieronder gegeven item kan informatie worden opgevraagd bij Verwerker.

Kruis aan als Verwerker voldoet, geef toelichting als niet voldoet:

- ☐ op risico gebaseerde aanpak beveiligingsmaatregelen
- ☐ beveiliging autorisatie en authenticatie
- ☐ rol en rechten structuur
- ☐ least privilige beginsel
- ☐ logging toegang en mutaties
- ☐ bewaartermijn loggegevens
- ☐ toegang tot logs voor Verantwoordelijke
- ☐ definitie datalek en zorgincident
- ☐ interne escalatieprocedure
- ☐ meldtermijnen, 24/7 meldpunt
- ☐ beschikbaarheidseisen
- ☐ back-up en herstel
- ☐ uitwijk en fallbackvoorziening
- ☐ change management
- ☐ impact analyse bij updates (testen voorafgaand productie)
- ☐ inzage relevante rapportages
- ☐ personeel (schriftelijke geheimhouding, screening, bewustwording)
- ☐ Conclusie: passende technische en organisatorische maatregelen?

Bijlage 3: Proces datalekken

Dit proces beschrijft het handelen van Verwerker rondom het melden van Datalekken en de te verstrekken informatie in combinatie met artikel 8 van de Verwerkersovereenkomst. Om Verantwoordelijke in staat te stellen correct aan haar AVG verplichtingen te voldoen, zal Verwerker direct na ontdekking van een (mogelijk) datalek, doch uiterlijk binnen 24 uur, Verantwoordelijke tenminste informeren over:

1. **Geef een samenvatting van het beveiligingslek/ beveiligingsincident/ datalek (tezamen "beveiligingsincident"): wat is er gebeurd?**
   Specificeer dit op basis van de laatst bekende informatie. Vermeld hier ook de naam van de betrokken systeem/systemen.

2. **Wat is het (vooralsnog bekende en/of te verwachten) gevolg?**
   Specificeer dit op basis van de laatst bekende informatie.

3. **Welke typen persoonsgegevens zijn betrokken bij het beveiligingsincident?**
   Maak een onderscheid tussen reguliere gegevens (zoals bijv. NAW, IP-adres en contactgegevens), gevoelige gegevens (zoals bijv. BSN, financiën of HR-dossiers) en bijzondere gegevens (zoals bijv. medische dossiers, behandelgegevens of informatie over de mentale gezondheid).

4. **Van hoeveel personen zijn de persoonsgegevens betrokken bij het beveiligingsincident?**
   Geef een minimum en maximum aantal getroffen personen aan.

5. **Omschrijving groep personen om wiens gegevens het gaat.**
   Bijzondere aandacht verdienen gegevens van een kwetsbare groepen personen, zoals kinderen of andere kwetsbaren.

6. **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?

7. **Wat is de oorzaak (root-cause) van het beveiligingsincident of datalek?**
   Specificeer dit op basis van de laatst bekende informatie.

8. **Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden?**
   Geef dit zo specifiek mogelijk aan.

9. **Welke maatregelen zijn er reeds getroffen of worden voorgesteld om de negatieve gevolgen te beperken en herhaling te voorkomen?**
   Specificeer dit op basis van de laatst bekende informatie.

Waar meld je het beveiligingsincident?

Als een (mogelijk) beveiligingsincident is ontdekt, neem direct contact op met de Privacy Officer:

Privacy Officer
E-mail: privacyofficer@ggdru.nl
Tel: 030-6086086

Functionaris Gegevensbescherming
E-mail: fg@ggdru.nl
Tel: 030-6086086