Verwerkersovereenkomst ARBIT-2016

Contractnummer: 201600274.003.127_A

De ondergetekenden:

1. Directie Organisatie, Bedrijfsvoering en Personeel, onderdeel van het Ministerie van Volksgezondheid, Welzijn en Sport, gevestigd te Den Haag,
te dezen vertegenwoordigd door (10)(2e) Directie Organisatie, Bedrijfsvoering en Personeel, de (10)(2e)
hierna te noemen: **Verwerkingsverantwoordelijke**,

en

2. Archie Europe BV,
gevestigd te Purmerend,
te dezen vertegenwoordigd door
H. van Bommel, algemeen directeur
hierna te noemen: **Verwerker**,

hierna gezamenlijk te noemen: **Partijen**;

OVERWEGENDE DAT:

- in het kader van de Dienstverlening door Verwerker, via de broker Protinus aan Verwerkingsverantwoordelijke Persoonsgegevens in de zin van artikel 4, onderdeel 1, van de Verordening worden verwerkt;
- artikel 28, derde lid, van de Verordening ertoe verplicht dat de Verwerking wordt geregeld in een overeenkomst of andere rechtshandeling die Verwerker ten aanzien van Verwerkingsverantwoordelijke bindt;
- Partijen in deze Verwerkersovereenkomst, zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Verwerker wensen vast te leggen.

KOMEN OVEREEN:

Artikel 1. Begrippen

In deze Verwerkersovereenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan wordt gegeven in artikel 1 van de Algemene Rijksvoorwaarden bij IT-overeenkomsten 2018 (ARBIT-2018). In afwijking daarvan of in aanvulling daarop wordt onder de volgende begrippen in deze Verwerkersovereenkomst verstaan:

1.1 Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.

1.2 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.

1.3 Overeenkomst: de overeenkomst tussen Verwerkingsverantwoordelijke en Verwerker inzake gebruiksrecht Archie met kenmerk 201600274.003.127.

1.4 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Verwerker in het kader van de Overeenkomst ten behoeve van Verwerkingsverantwoordelijke verwerkt.

1.5 Verordening: 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 en tot intrekking van de Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

1.6 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

1.7 Verwerking: een bewerking of een geheel van bewerkingen in het kader van de Overeenkomst 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, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen.

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Verwerker in het kader van de Overeenkomst.

2.2 De aard en het doel van de Verwerking, het soort Persoonsgegevens en de categorieën van Persoonsgegevens, Betrokkenen en ontvangers zijn in Bijlage 1 omschreven.

2.3 Verwerker garandeert de toepassing van passende technische en organisatorische maatregelen, opdat de Verwerking aan de vereisten van de Verordening voldoet en de bescherming van de rechten van de Betrokkene is gewaarborgd.

2.4 Verwerker garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

Artikel 3. Inwerkingtreding en duur

3.1 Deze Verwerkersovereenkomst treedt in werking op het moment waarop deze door Partijen is ondertekend.

3.2 Deze Verwerkersovereenkomst eindigt nadat en voor zover Verwerker alle Persoonsgegevens overeenkomstig artikel 10 heeft gewist of terugbezorgd.

3.3 Geen van Partijen kan deze Verwerkersovereenkomst tussentijds opzeggen.

Artikel 4. Omvang verwerkingsbevoegdheid Verwerker

4.1 Verwerker verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van Verwerkingsverantwoordelijke behoudens afwijkende wettelijke voorschriften die op Verwerker van toepassing zijn.

4.2 Indien een instructie als bedoeld in het eerste lid naar het oordeel van Verwerker in strijd is met een wettelijk voorschrift inzake gegevensbescherming, stelt hij

Verwerkingsverantwoordelijke daarvan voorafgaand aan de Verwerking in kennis, tenzij een wettelijk voorschrift deze kennisgeving verbiedt.

4.3 Indien Verwerker op grond van een wettelijk voorschrift Persoonsgegevens dient te verstrekken, informeert hij Verwerkingsverantwoordelijke onmiddellijk, en zo mogelijk voorafgaand aan de verstrekking.

4.4 Verwerker heeft geen zeggenschap over het doel van en de middelen voor de Verwerking van Persoonsgegevens.

Artikel 5. Beveiliging van de Verwerking

5.1 In aanvulling op artikel 19 van de ARBIT-2018 en onverminderd artikel 2.3 treft Verwerker de technische en organisatorische beveiligingsmaatregelen zoals beschreven in Bijlage 2.

5.2 Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Verwerker waarborgt een op het risico afgestemd beveiligingsniveau.

5.3 Indien en voor zover Verwerkingsverantwoordelijke daarom uitdrukkelijk schriftelijk verzoekt, zal Verwerker aanvullende maatregelen treffen met het oog op de beveiliging van de Persoonsgegevens.

5.4 Verwerker verwerkt Persoonsgegevens niet buiten de Europese Unie, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Verwerkingsverantwoordelijke en behoudens afwijkende wettelijke verplichtingen.

5.5 Verwerker informeert Verwerkingsverantwoordelijke zonder onredelijke vertraging zodra hij kennis heeft genomen van onrechtmatige Verwerkingen van Persoonsgegevens of inbreuken op beveiligingsmaatregelen zoals genoemd in het eerste en tweede lid.

5.6 Verwerker verleent Verwerkingsverantwoordelijke bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de Verordening.

Artikel 6. Geheimhouding door Personeel van Verwerker

6.1 De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 17.1 van de ARBIT-2018.

6.2 Verwerker toont op verzoek van Verwerkingsverantwoordelijke aan dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 17.2 van de ARBIT-2018.

Artikel 7. Subverwerker

Wanneer Verwerker, met inachtneming van het bepaalde in artikel 23 van de ARBIT-2018, een andere verwerker inschakelt om ten behoeve van Verwerkingsverantwoordelijke verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in deze Verwerkersovereenkomst zijn opgenomen.

Artikel 8. Bijstand vanwege rechten van Betrokkene

Verwerker verleent Verwerkingsverantwoordelijke bijstand bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III van de Verordening vastgelegde rechten van de Betrokkene te beantwoorden.

Artikel 9. Inbreuk in verband met Persoonsgegevens

9.1 Verwerker informeert Verwerkingsverantwoordelijke zonder onredelijke vertraging, zodra hij kennis heeft genomen van een Inbreuk in verband met Persoonsgegevens, overeenkomstig de afspraken zoals vastgelegd in Bijlage 3.

9.2 Verwerker informeert Verwerkingsverantwoordelijke ook na een melding op grond van het eerste lid over ontwikkelingen betreffende de Inbreuk in verband met Persoonsgegevens.

9.3 Partijen dragen elk de door henzelf in verband met de melding aan de bevoegde toezichthoudende autoriteit en Betrokkene te maken kosten.

Artikel 10. Terugbezorgen of wissen Persoonsgegevens

10.1 Na afloop van de Overeenkomst draagt Verwerker, naar gelang de keuze van Verwerkingsverantwoordelijke, zorg voor het terugbezorgen aan Verwerkingsverantwoordelijke of het wissen van alle Persoonsgegevens. Verwerker verwijdert kopieën, behoudens afwijkende wettelijke voorschriften.

Artikel 11. Informatieverplichting en audit

11.1 Verwerker stelt alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst zijn en worden nagekomen.

11.2 Verwerker verleent alle benodigde medewerking aan audits.

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

Den Haag, ... - ... - 2019	Den Haag, ... - ... - 2019
Ministerie van Volksgezondheid, Welzijn en Sport	Archie Europe BV
namens deze, (10)(2e)	namens deze, Algemeen Directeur,
(10)(2e)	H. van Bommel

Bijlage 1. De Verwerking van Persoonsgegevens

Onderwerp Verwerking/Soort Persoonsgegevens:
De verwerking van persoonsgegevens heeft betrekking op het gebruik van Archie CRM.
In de applicatie worden persoonsgegevens van gebruikers opgeslagen.
De volgende persoonsgegevens van een gebruiker worden verwerkt:

- Voornaam
- Achternaam
- E-mailadres
- Rechten in de applicatie
- Gebruikersnaam
- Wachtwoord

De gebruikers van Archie CRM bepalen uiteindelijk zelf welke persoonsgegevens zij verwerken.
De verwerking van persoonsgegevens is afhankelijk van hetgeen de Verwerkingsverantwoordelijke in de applicatie opneemt maar bestaat in de meeste gevallen uit de verwerking van:

- Naam
- E-mailadres
- Organisatie
- CRM Invoergegevens
- Mailwisseling

Verwerkingsverantwoordelijke zal geen persoonsgegevens zoals bedoeld in artikel 9 en 10 van de AVG, Burgerservicenummers (BSN) of persoonsgegevens van kinderen jonger dan 16 jaar (laten) verwerken in Archie CRM.

Duur:
De Verwerkingsverantwoordelijke heeft volledige zeggenschap over de duur van de verwerking en de opslag van gegevens. Verwerker zal persoonsgegevens niet langer bewaren dan benodigd voor de verlening van de door Verwerkingsverantwoordelijke verzochte dienst of benodigd om te voldoen aan de doelen waarvoor de persoonsgegevens zijn verstrekt.

Aard en Doel:
Verwerker verricht de volgende verwerkingen van persoonsgegevens voor de Verwerkingsverantwoordelijke:

- Opslag.

De doeleinden waarvoor de persoonsgegevens verwerkt zullen worden:

- Onderhouden contacten
- Opslag en uitwisseling correspondentie binnen projectteam

Categorieën Van Betrokkenen:
Werknemers en [adviseurs] Eén tegen eenzaamheid.

Bijlage 2. Passende technische en organisatorische maatregelen

In geval dat Archie Europe BV optreedt als Verwerker, geldt in elk geval dat conform de rijksbrede afspraken de BIO (Baseline Informatiebeveiliging Overheid) zal worden toegepast.

Tevens treft verwerker de volgende maatregelen:

Beveiligingsmaatregelen hostingomgeving

- Archie Europe hanteert een autorisatiebeleid voor de Archie CRM hostingomgeving om te zorgen dat medewerkers alleen toegang hebben tot de informatie die strikt noodzakelijk is om hun werkzaamheden te verrichten.
- Toegangsrechten worden geregistreerd.
- Registratie van service accounts en andere beveiligingscredentials anders dan de persoonlijke logins geschiedt in een beveiligde database.
- Alleen specifieke medewerkers hebben toegang tot de beveiligde database, kluizen (via Fingerprint), sleutels etc. waar zich informatie bevindt die toegang kan geven tot de cloudservers en/of data van klanten.
- Alleen een specifieke medewerker is (al dan niet in opdracht van de security/privacy officer) bevoegd om een gebuikersidentificatie af te geven/aan te maken.
- Er worden periodiek versleutelde back-ups gemaakt van de data in de Archie hostingomgeving ten behoeve van de continuïteit van de dienstverlening welke vertrouwelijk worden behandeld en bewaard in een zowel fysiek als virtueel beveiligde omgeving. Deze worden fysiek op een andere locatie bewaard. Daarnaast is er een beveiligde failover omgeving beschikbaar op een derde locatie.
- De inzet van de AMEE laag (Archie Multi-Tier Environment Engine – tussenlaag software) beschermt de Archie database op de SQL server doordat Archie gebruikers via de client nooit rechtstreeks verbinding maken met de SQL server. De communicatie met de database wordt afgehandeld via geregistreerde SQL gebruiker (username en password zoals geregistreerd binnen de SQL server omgeving). Het Client-Server verkeer is versleuteld volgens de AES standaard. Het web verkeer is versleuteld middels een SSL certificaat.
- De netwerkomgeving waarbinnen data wordt verwerkt is strikt beveiligd. Op wachtwoorden worden cryptografische maatregelen toegepast en verkeersstromen worden gescheiden.
- De beveiliging van de omgeving waarbinnen persoonsgegevens in de hostingomgeving van Archie worden verwerkt wordt gemonitord.
- Op de systemen worden periodiek de laatste (beveiliging)patches geïnstalleerd op basis van patchmanagement.
- Er wordt jaarlijks een Pen- en Hacktest uitgevoerd door een gespecialiseerd bureau zodat de meest actuele beveiligingsverbeteringen kunnen worden geïmplementeerd.

Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens

De volgende afspraken zijn van toepassing op de Verwerker en Verwerkingsverantwoordelijke met betrekking tot het afhandelen van informatiebeveiliging-incidenten waaronder datalekken:

Definitie informatiebeveiliging-incident (IB-incident): "Onbedoelde gebeurtenis die tot schade op informatie heeft geleid of zou kunnen leiden".

Definitie datalek: "een informatiebeveiliging-incident waarbij persoonsgegevens verloren zijn gegaan, of een onrechtmatige verwerking redelijkerwijs niet is uit te sluiten".

Voor het melden van incidenten dient de volgende procedure te worden gevolgd:

- De Verwerker zal de Verwerkingsverantwoordelijke zo spoedig mogelijk, doch uiterlijk binnen 24 uur na de eerste ontdekking van het IB-incident, informeren over alle inbreuken op de beveiliging alsmede andere incidenten die op grond van wetgeving moeten worden gemeld aan een toezichthouder of betrokkene, onverminderd de verplichting de gevolgen van dergelijke inbreuken en incidenten zo snel mogelijk ongedaan te maken dan wel te beperken.

- Direct na het constateren van een IB-Incident, wordt deze door de Verwerker per e-mail gemeld aan de Verwerkingsverantwoordelijke op het volgende e-mail adres (10)(2e)@minvws.nl en contactpersoon. Ook wordt buiten kantooruren de Beveiligingsambtenaar (BVA) telefonisch ingelicht.

- De Verwerker neemt in de melding in ieder geval de volgende gegevens op:

    - **Contactgegevens melder**
        - Naam, e-mail, telefoonnummer, functie, organisatie en organisatieonderdeel.
    - **Gegevens over het IB-incident**
        - IB-incident-id; het kenmerk van het IB-incident.
        - Een korte omschrijving van het IB-incident met daarin een samenvatting van wat zich heeft voorgedaan.
        - Classificatie IB-incident (Kritiek, Hoog, Midden, Laag, Zeer laag) (zie IB-Incident-classificatiemodel)
            - Urgentie (Hoog, Midden, Laag) (zie IB-incidenturgentiemodel);
            - Impact (Hoog, Midden, Laag) (zie IB-incidentimpactmodel); bereik incident: aantal mensen, deel infrastructuur.
        - Het tijdstip van de gebeurtenis.
            a) Op (dag, maand, jaar, uur en minuut) zo precies mogelijk.
            b) Tussen begindatum periode en einddatum periode.
            c) Onbekend.
        - Het tijdstip van ontdekking:
            a) Op (dag, maand, jaar, uur en minuut) zo precies mogelijk.
            b) Tussen begindatum periode en einddatum periode.
            c) Onbekend.
        - Typeer het IB-Incident hoofdoorzaak
            a) Verlies van informatiedragers (o.a. telefoon, tablet, usb-stick, dossier)
            b) Diefstal van informatiedragers
            c) Diefstal van informatie
            d) Aanval op personen (social engineering: o.a. phishing, bedreiging etc.)
            e) Aanval op ICT-middelen (o.a. malware, cryptolocker, etc.)
            f) Uitval van ICT-middelen (o.a. denial-of-service, brand, etc.)
            g) Ongeoorloofde toegang tot informatie (o.a. door identiteitsfraude, inbraak, autorisatiefouten etc.)
            h) Ongeoorloofd gebruik van informatie (onrechtmatig verstrekken, wijzigen, vernietigen etc.)
            i) Ongeoorloofd gebruik van ICT-middelen

- Toelichting op typering (omschrijving van het wie, wat, waar en hoe het heeft plaatsgevonden en de gevolgen)
- Vertrouwelijkheid melding
- Soort schade
    a) Reputatie-schade (via waarde schaal: Hoog-Midden-Laag-Geen)
    b) Financiële-schade (in euro's of via waarde schaal: Hoog-Midden-Laag-Geen)
    c) Persoonsgegevens (Datalek) (ja/nee) bij ja, vul het onderstaande in.
        - Van hoeveel personen zijn Persoonsgegevens betrokken bij de inbreuk? (Vul de aantallen in):
            - Minimaal:
            - Maximaal:
        - Omschrijf de groep mensen van wie Persoonsgegevens zijn betrokken bij de inbreuk.
        - Wat is de aard van de inbreuk? *(meerdere opties mogelijk)*
            - Lezen (vertrouwelijkheid)
            - Kopiëren
            - Veranderen (integriteit)
            - Verwijderen of vernietigen (beschikbaarheid)
            - Diefstal
            - Nog niet bekend
        - Om welk type Persoonsgegevens gaat het? Over te nemen uit bijlage 1 Gegevens van betrokkenen. *(meerdere opties mogelijk)*
        - Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen? *(meerdere opties mogelijk)*
            - Stigmatisering of uitsluiting
            - Schade aan de gezondheid
            - Blootstelling aan (identiteits)fraude
            - Blootstelling aan spam of phishing
            - Anders, namelijk (vul aan)
        - Zijn de Persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden? (Kies een van de volgende opties en vul waar nodig aan.)
            - Ja
            - Nee
            - Deels, namelijk: (vul aan)
        - Als de Persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? (Beantwoord deze vraag als u bij de vorige vraag gekozen heeft voor optie a of optie c. Als u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.)
        - Heeft de inbreuk betrekking op personen in andere EU-landen? (Kies een van de volgende opties.)
            - Ja
            - Nee
            - Nog niet bekend
- Leden incident-response team

Tijdens het incident worden de volgende punten van de acties of maatregelen bijgehouden:
- Datum en tijd;
- Betrokken partij
- Beschrijving van de genomen maatregel of actie;

Vervolgacties naar aanleiding van het IB-incident
Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

IB-incidenturgentiemodel

De urgentie wordt als volgt gedefinieerd:

Categorie	Applicatie	Schade
Hoog	Een vitale applicatie wordt geraakt door het incident tijdens een kritiekmoment.	De schade veroorzaakt door het incident neemt snel toe. Werk dat moet worden hersteld door personeel is zeer arbeidsintensief.
Midden	Een vitale applicatie wordt geraakt door het incident./ Een ondersteunende applicatie wordt geraakt tijdens een kritiekmoment	De schade veroorzaakt door het incident neemt in de tijd aanzienlijk toe. Er gaat werk verloren, maar dit is relatief snel te herstellen.
Laag	Een van de ondersteunende applicatie wordt geraakt.	De schade veroorzaakt door het incident neemt in de tijd maar weinig toe. Het werk dat blijft liggen is niet tijdsintensief.

De hoogst geclassificeerde categorie wordt gebruikt in het bepalen van de urgentie.

IB-incidentimpactmodel

De impact wordt als volgt gedefinieerd:

Categorie	Vertrouwelijk-heid	Reikwijdte	Eind-gebruikers	Reputatie	SLA
Hoog	Het incident betreft zeer vertrouwelijke gegevens STG. /WBP III.	De gehele dienst-verlening wordt beïnvloed.	Relatief veel eind-gebruikers zijn is geraakt door het incident en/of kan zijn/haar werk niet meer doen. Meerdere afdelingen zijn geraakt.	Er is reputatie-schade, de krant wordt gehaald.	De dienst-verlening zoals afgesproken in de SLA is stil komen te liggen.
Midden	Het incident betreft vertrouwelijke gegevens DEP-V/ WBP II-I.	Een deel van de dienst-verlening worden geraakt.	Enig eind-gebruikers zijn geraakt door het incident en/of kan zijn/haar werk niet meer doen, bijvoorbeeld een afdeling.	Er is kans op reputatie-schade.	De dienst-verlening zoals afgesproken in de SLA wordt in grote mate negatief beïnvloed door het incident
Laag	Het betreft niet vertrouwelijk gegevens openbaar/WBP 0.	Enkele personen in het service-gebied worden geraakt.	Enkele eind-gebruikers zijn geraakt door het incident en/of kunnen niet meer hun werk doen.	Er is geen kans op reputatie-schade.	De dienst-verlening zoals afgesproken in de SLA wordt minimaal beïnvloed door het incident

De hoogst geclassificeerde categorie wordt gebruikt in het bepalen van de impact.

IB-Incident-meldingsmodel
Prioriteit:

	Impact Hoog	Impact Midden	Impact Laag
Urgentie Hoog	1	2	3
Urgentie Midden	2	3	4
Urgentie Laag	3	4	5

IB-Incident-classificatiemodel
Nadat de melding een prioriteit heeft gekregen kan de cmelding geclassificeerd worden en zijn de gewenste reactietijd en afhandeltijd bekend.

Code	Omschrijving	Reactietijd	Maximale oplossingstijd
1	Kritiek	Onmiddellijk	1 uur
2	Hoog	10 minuten	4 uur
3	Midden	1 uur	8 uur
4	Laag	4 uur	24 uur
5	Zeer laag	1 dag	1 week

Na de inschaling is bekend welke capaciteit gebruikt mag worden voor het oplossen van het incident. Hieruit wordt een incidentresponseteam samengesteld. Dit kan per incident verschillen afhankelijk van de oorzaak en de gevolgen van het incident.

Code	Bedrijfsonderdeel	Leverancier	Afdeling beveiliging	dCO
Kritiek	AIB,FB	AB,TB	ISO, CISO, BVA,	(10)(2e)
Hoog	AIB,FB	AB,TB	ISO, CISO	Medw. Comm
Midden	AIB,FB 2	AB	ISO	Medw. Comm
Laag	AIB,FB 1	AB 1		Medw. Comm
Zeer laag	AIB,FB 1			

Uitgangspunten:

- De Verwerker zal het doen van meldingen aan de toezichthouder(s) overlaten aan de Verwerkingsverantwoordelijke.
- De Verwerker zal alle noodzakelijke medewerking verlenen aan het zo nodig, op de kortst mogelijke termijn, verschaffen van aanvullende informatie aan de toezichthouder(s) en/of betrokkene(n).
- De Verwerker houdt een gedetailleerd logboek bij van alle inbreuken op de beveiliging, evenals de maatregelen die in vervolg op dergelijke inbreuken zijn genomen, en geeft daar op eerste verzoek van de verantwoordelijke inzage in.
- De Verwerkingsverantwoordelijke heeft het recht om eigen onderzoek uit te laten voeren waaraan de Verwerker volledige medewerking zal verlenen.
- De Verwerker neemt alle passende technische en organisatorische maatregelen om de persoonsgegevens welke worden verwerkt ten dienste van de Verwerkingsverantwoordelijke te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van onzorgvuldig, ondeskundig of ongeoorloofd gebruik.
- Na het afronden van de melding, kan de Verwerkingsverantwoordelijke de Verwerker een opdracht verstrekken voor het nemen van aanvullende maatregelen.