# Verwerkersovereenkomst dienstverlening Mickcom ICT

## Inleiding

**Verantwoordelijke en verwerker**

In de privacy regelgeving, zoals de Wet bescherming persoonsgegevens (Wbp) wordt onderscheid gemaakt tussen verantwoordelijke en een verwerker. De verantwoordelijke is degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt en de verwerker degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen. Iedere organisatie verwerkt voor eigen doeleinden persoonsgegevens, zoals de eigen klantenadministratie, financiële administratie of personeelsadministratie. Voor deze verwerkingen is de organisatie de verantwoordelijke. Als een dienstverlener voor derden persoonsgegevens verwerkt, zoals een administratiekantoor of een cloud dienstverlener, dan geldt deze dienstverlener voor deze verwerkingen als verwerker ten opzichte van de opdrachtgever. De verantwoordelijke dient aan de volledige privacy regelgeving te voldoen. De verwerker moet zich met name houden aan de (schriftelijke) aanwijzingen van de verantwoordelijke en mag de persoonsgegevens niet voor eigen doeleinden gebruiken. Overigens is het onderscheid lang niet altijd eenduidig en kan een verwerker in bepaalde gevallen tevens verantwoordelijke of medeverantwoordelijke zijn. Als een verwerker voor eigen doeleinden de persoonsgegevens verwerkt die hij heeft verkregen in het kader van zijn dienstverlening aan derden - bijvoorbeeld voor het maken van analyses ter verbetering van zijn eigen dienstverlening - geldt de verwerker voor die verwerking als verantwoordelijke.

**Wettelijke verplichting**

Indien een organisatie (ICT)werkzaamheden uitbesteedt waarbij persoonsgegevens worden verwerkt door de dienstverlener, zoals bijvoorbeeld de cloud werkplek, zal de uitbestedende organisatie een verwerkersovereenkomst moeten sluiten met de dienstverlener. Deze verplichting vloeit voort uit artikel 14 lid 2 en lid 3 Wbp. De Autoriteit Persoonsgegevens (dan wel College Bescherming Persoonsgegevens) heeft in hoofdstuk 4.2 van de CBP Richtsnoeren Beveiliging van Persoonsgegevens aangegeven welke afspraken in ieder geval in een verwerkersovereenkomst dienen te worden opgenomen.

 

# Inhoudsopgave


Inleiding ..... 1

Inhoudsopgave ..... 2

VERWERKERSOVEREENKOMST ..... 3

Artikel 1. Definities ..... 4

Artikel 2. Algemeen ..... 6

Artikel 3. Verwerken van Persoonsgegevens ..... 6

Artikel 4. Geheimhouding ..... 6

Artikel 5. Beveiliging Persoonsgegevens ..... 7

Artikel 6. Controle ..... 8

Artikel 7. Beveiligingsincidenten ..... 8

Artikel 8. Verzoeken van Betrokkenen ..... 9

Artikel 9. Sub-verwerkers ..... 9

Artikel 10. Toegang tot de Persoonsgegevens ..... 9

Artikel 11. Aansprakelijkheid en vrijwaring ..... 10

Artikel 12. Duur en beëindiging ..... 10

Artikel 13. Wijziging Verwerkersovereenkomst ..... 11

Artikel 14. Toepasselijk recht / Bevoegde rechter ..... 11

BIJLAGE 1 ..... 12

BIJLAGE 2 ..... 13

BIJLAGE 3 “Procedure Meldplicht Datalekken” ..... 14

Vragenlijst Beveiligingsincident – bij de Procedure Meldplicht Datalekken ..... 15


 

# VERWERKERSOVEREENKOMST

**Partijen**:

**1.** De persoon of rechtsvorm welke diensten afneemt bij Mickcom ICT, hierna te noemen "**VERANTWOORDELIJKE**";

en

**2.** Mickcom ICT gevestigd aan de Platinastraat 10-K hierna te noemen "**VERWERKER**"

hierna gezamenlijk te noemen: 'Partijen'

**OVERWEGENDE DAT**

a. VERWERKER in het kader de uitvoering van de diensten ook Persoonsgegevens verwerkt voor VERANTWOORDELIJKE.

b. Dat partijen wettelijk verplicht zijn afspraken te maken en vast te leggen met betrekking tot de verwerking van Persoonsgegevens door VERWERKER.

c. De bepalingen van deze Verwerkersovereenkomst vóór gaan op alle andere afspraken die tussen Partijen gelden en betrekking hebben op de verwerking van Persoonsgegevens door VERWERKER voor VERANTWOORDELIJKE.

**KOMEN ALS VOLGT OVEREEN:**

## Artikel 1. Definities

Naast de wettelijke definities hebben de volgende termen de volgende betekenis:

| | |
|---|---|
| “AP” | Autoriteit Persoonsgegevens, ook College Bescherming Persoonsgegevens genoemd, de toezichthoudende autoriteit voor de naleving van de geldende privacywetgeving; |
| “AVG” | Algemene Verordening Gegevensbescherming, voluit: Verordening (EU) 2016/679 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 Richtlijn 95/46/EG; |
| “Betrokkene” | de natuurlijke persoon waarop de Persoonsgegevens die VERWERKER verwerkt voor VERANTWOORDELIJKE en/of haar opdrachtgevers in het kader van de uitvoering van de Overeenkomst betrekking hebben; |
| “Beveiligingsincident” | 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 Persoonsgegevens; |
| “Verwerkersovereenkomst” | de onderhavige overeenkomst inclusief alle bijlagen die onlosmakelijk hieraan zijn verbonden; |
| “Bijlage” | Iedere bijlage bij deze Verwerkersovereenkomst, welke een onlosmakelijk deel daarvan uitmaakt; |
| "Derde" | een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de Betrokkene, noch de Verantwoordelijke, noch de Verwerker, noch de personen die onder rechtstreeks gezag van de Verantwoordelijke of de verwerker gemachtigd zijn om de Persoonsgegevens te verwerken; |
| “Diensten” | Alle diensten die VERWERKER aan VERANTWOORDELIJKE verleent, zoals omschreven in de Overeenkomst; |
| “EER” | Europese Economische Ruimte; |

| | |
|---|---|
| “Persoonsgegevens” | alle informatie over een geïdentificeerde of identificeerbare<br><br>natuurlijke persoon die VERWERKER ontvangt van of verwerkt voor VERANTWOORDELIJKE in het kader van de uitvoering van de Overeenkomst; |
| “Sub-verwerker” | een partij die door VERWERKER wordt ingeschakeld voor de uitvoering van de Overeenkomst en de daarbij horende verwerking van Persoonsgegevens; |
| “Wbp” | Wet bescherming persoonsgegevens; |
| “Verwerken” | elke handeling of elk geheel van handelingen met betrekking tot Persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens; |

## Artikel 2. Algemeen

2.1 VERANTWOORDELIJKE wordt ten aanzien van de Persoonsgegevens beschouwd als Verantwoordelijke in de zin van de Wbp en Verwerkingsverantwoordelijke in de zin van de AVG. VERWERKER is Verwerker in de zin van de Wbp en Verwerker in de zin van de AVG.

2.2 VERWERKER en VERANTWOORDELIJKE verstrekken elkaar over en weer tijdig alle benodigde informatie om een goede naleving van de geldende privacywet- en regelgeving mogelijk te maken.

## Artikel 3. Verwerken van Persoonsgegevens

3.1 De producten en diensten van VERWERKER zijn in basis geschikt voor de verwerking van persoonsgegevens. Hierbij is geen rekening gehouden met handelingen die door Opdrachtgever worden uitgevoerd nadat het product of de dienst door VERWERER is opgeleverd; het aanpassen van instellingen, installeren (en/of foutief configureren) van software et cetera kan een beveiligingsrisico opleveren. Voor dergelijke zaken waar VERWERKER geen invloed op heeft, ligt de verantwoordelijkheid uitsluitend bij VERANTWOORDELIJKE. Bij de producten en diensten van VERWERKER is geen rekening gehouden met de verwerking van bijzondere persoonsgegevens, of om gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten mee te verwerken. Verwerken van deze gegevens met de producten en diensten van VERWERKER door VERANTWOORDELIJKE is ter eigen beoordeling door VERANTWOORDELIJKE.

3.2 VERANTWOORDELIJKE zal de Persoonsgegevens in overeenstemming met de geldende wet- en regelgeving verwerken. VERWERKER zal de Persoonsgegevens niet voor andere doeleinden of op andere wijze gebruiken dan voor het doel waarvoor de Persoonsgegevens zijn verstrekt of haar bekend zijn geworden.

3.3 VERWERKER zal de Persoonsgegevens uitsluitend verwerken op basis van de schriftelijke instructies van VERANTWOORDELIJKE in het kader van de uitvoering van de Overeenkomst en de verleende Diensten, dan wel in verband met een wettelijke verplichting.

3.4 VERWERKER zal de Persoonsgegevens niet aan een Derde verstrekken, tenzij deze uitwisseling plaatsvindt in opdracht van VERANTWOORDELIJKE in het kader van de uitvoering van de Overeenkomst of wanneer dit noodzakelijk is om te voldoen aan een wettelijke verplichting.

3.5 VERWERKER draagt er zorg voor dat de Persoonsgegevens niet buiten de EER worden verwerkt, tenzij VERANTWOORDELIJKE daar schriftelijke toestemming voor heeft gegeven.

## Artikel 4. Geheimhouding

4.1 VERWERKER houdt de Persoonsgegevens die zij verwerkt in het kader van de uitvoering van de Overeenkomst geheim en zal alle nodige maatregelen treffen om geheimhouding van de

Persoonsgegevens te verzekeren. VERWERKER zal de verplichting tot geheimhouding tevens opleggen aan haar personeel en alle door haar ingeschakelde personen.

4.2 De in dit artikel bedoelde geheimhoudingsplicht geldt niet indien VERANTWOORDELIJKE uitdrukkelijk schriftelijk toestemming heeft gegeven om de Persoonsgegevens aan een Derde te verstrekken, of een wettelijke verplichting bestaat om de Persoonsgegevens aan een Derde te verstrekken.

## Artikel 5. Beveiliging Persoonsgegevens

5.1 VERANTWOORDELIJKE zal in overeenstemming met de geldende wettelijke regels de beveiliging van de Persoonsgegevens waarborgen en daartoe passende technische en organisatorische maatregelen treffen.

5.2 VERWERKER zal in overeenstemming met de geldende wettelijke regels technische en organisatorische maatregelen treffen, in stand houden en zo nodig aanpassen om een op het risico afgestemd beveiligingsniveau te waarborgen. Om hieraan te kunnen voldoen zal VERANTWOORDELIJKE VERWERKER informeren over de betrouwbaarheidseisen die op de verwerking van toepassing zijn en tijdig de benodigde informatie verstrekken in geval van wijzigingen in de verwerking van Persoonsgegevens.

5.3 VERWERKER zal bij het treffen van beveiligingsmaatregelen rekening houden 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.

5.4 Indien VERANTWOORDELIJKE een beoordeling wenst uit te voeren van een beoogde verwerkingsactiviteit in het kader van de uitvoering van de Overeenkomst zal VERWERKER alle redelijke medewerking verlenen om deze beoordeling in overeenstemming met de geldende wet- en regelgeving uit te kunnen voeren. Tevens zal VERWERKER alle redelijke medewerking verlenen indien een voorafgaande raadpleging van de AP nodig is op grond van de geldende privacywetgeving. VERANTWOORDELIJKE zal VERWERKER de in dit kader gemaakte redelijke kosten vergoeden.

5.5 In **Bijlage 2** zijn de afspraken tussen Partijen vastgelegd over de concrete technische en organisatorische beveiligingsmaatregelen die VERWERKER treft. Deze maatregelen worden periodiek geëvalueerd en indien nodig aangepast. Verwerkingsverantwoordelijke erkent dat zij de in **Bijlage 2** opgenomen afspraken voldoende acht voor een passende beveiliging van de Persoonsgegevens in overeenstemming met de geldende wettelijke verplichtingen.

## Artikel 6. Controle

6.1 In geval van een onderzoek door de AP of een andere bevoegde autoriteit zal VERWERKER alle redelijke medewerking verlenen en VERANTWOORDELIJKE zo snel mogelijk informeren. Partijen zullen met elkaar in overleg treden over de wijze van optreden en de verdeling van de kosten.

## Artikel 7. Beveiligingsincidenten

7.1 VERWERKER informeert VERANTWOORDELIJKE onverwijld nadat VERWERKER kennis heeft genomen van een Beveiligingsincident met betrekking tot de verwerking van de Persoonsgegevens.

7.2 In geval van een Beveiligingsincident zal VERWERKER alle redelijke maatregelen treffen om de gevolgen van het incident te beperken en/of een nieuw incident te voorkomen. VERWERKER zal alle medewerking verlenen aan VERANTWOORDELIJKE om het beveiligingsincident te beoordelen en te kunnen voldoen aan haar eventuele wettelijke meldplicht en haar eventuele plicht tot het informeren van Betrokkenen.

7.3 Partijen leggen hun afspraken over de informatie-uitwisseling in verband met incidenten vast in een “Procedure Meldplicht Datalekken” in **Bijlage 3**. Deze bijlage kan ten allen tijde in overleg door Partijen worden gewijzigd. De bijlage zal in ieder geval worden aangepast indien de regelgeving omtrent de Meldplicht Datalekken of de uitleg daarvan wijzigt.

7.4 In geval van een Beveiligingsincident bij VERWERKER dat leidt tot een meldplicht of een informatieplicht voor VERANTWOORDELIJKE, zal de melding of de informatieverstrekking in overleg met VERWERKER door VERANTWOORDELIJKE worden verricht. Partijen zullen in goed overleg afspraken maken over de verdeling van de kosten die daarmee zijn gemoeid.

## Artikel 8. Verzoeken van Betrokkenen

8.1 Indien VERWERKER een verzoek of bezwaar van een Betrokkene ontvangt, zoals een verzoek om informatie, inzage, rectificatie, gegevenswissing, verwerkingsbeperking, overdracht van de Persoonsgegevens, stuurt VERWERKER dat verzoek onmiddellijk door naar VERANTWOORDELIJKE.

8.2 VERWERKER verleent VERANTWOORDELIJKE alle redelijke medewerking om ervoor te zorgen dat VERANTWOORDELIJKE binnen de wettelijke termijnen kan voldoen aan de verplichtingen op grond van de geldende wet- en regelgeving. De redelijke kosten voor deze medewerking zullen door VERANTWOORDELIJKE aan VERWERKER worden vergoed.

## Artikel 9. Sub-verwerkers

9.1 VERWERKER heeft bij de verwerking van de Persoonsgegevens de mogelijkheid om, Sub-verwerkers in te schakelen.

9.2 VERWERKER zal met de door haar ingeschakelde Sub-verwerkers een overeenkomst sluiten die in overeenstemming is met de relevante wet- en regelgeving en deze Verwerkersovereenkomst. VERWERKER zal in ieder geval iedere Sub-VERWERKER contractueel de geheimhoudingsverplichtingen, meldingsverplichtingen en beveiligingsmaatregelen na laten leven met betrekking tot de verwerking van de Persoonsgegevens.

## Artikel 10. Toegang tot de Persoonsgegevens

10.1 De zeggenschap over de Persoonsgegevens blijft volledig berusten bij VERANTWOORDELIJKE. Op verzoek van VERANTWOORDELIJKE en tegen vergoeding van de redelijke kosten zal VERWERKER alle of een gedeelte van de Persoonsgegevens in gangbaar formaat ter beschikking stellen aan VERANTWOORDELIJKE.

10.2 VERWERKER zal ervoor zorgdragen dat VERANTWOORDELIJKE te allen tijde toegang behoudt tot de Persoonsgegevens en zal in geval van een geschil tussen Partijen deze toegang niet blokkeren.

## Artikel 11. Aansprakelijkheid en vrijwaring

11.1 Indien een Partij tekortschiet in de nakoming van de Verwerkersovereenkomst is deze Partij aansprakelijk voor de schade en kosten die de andere Partij daardoor lijdt of heeft geleden.

11.2 VERWERKER vrijwaart VERANTWOORDELIJKE voor boetes en/of dwangsommen van of namens de AP en/of andere bevoegde autoriteiten die aan VERANTWOORDELIJKE worden opgelegd en waarbij vast is komen te staan dat deze zijn toe te schrijven aan overtredingen van de geldende privacywetgeving door VERWERKER met in achtneming van de genoemde beperkingen in artikel 11.1. Om een beroep te kunnen doen op deze vrijwaring is VERANTWOORDELIJKE gehouden om:

(i) VERWERKER terstond op de hoogte te brengen van enig onderzoek of andere aanleiding die zou kunnen leiden tot een voornemen van een toezichthouder tot het opleggen van een boete of last onder dwangsom,

(ii) in samenspraak met VERWERKER te handelen en te communiceren richting de toezichthouder
én

(iii) tegen opgelegde boetes in bezwaar en/of beroep te gaan indien daar redelijkerwijs aanleiding voor is.

11.3 VERANTWOORDELIJKE vrijwaart VERWERKER voor boetes en/of dwangsommen van of namens de AP en/of andere bevoegde autoriteiten die aan VERWERKER worden opgelegd en waarbij vast is komen te staan dat deze zijn toe te schrijven aan overtredingen van de geldende privacywetgeving door VERANTWOORDELIJKE. Om een beroep te kunnen doen op deze vrijwaring is VERWERKER gehouden om:

(i) VERANTWOORDELIJKE terstond op de hoogte te brengen van enig onderzoek of andere aanleiding die zou kunnen leiden tot een voornemen van een toezichthouder tot het opleggen van een boete of last onder dwangsom,

(ii) in samenspraak met VERANTWOORDELIJKE te handelen en te communiceren richting de autoriteit
en

(iii) tegen opgelegde boetes in bezwaar en/of beroep te gaan indien VERANTWOORDELIJKE daar redelijkerwijs aanleiding voor is.

## Artikel 12. Duur en beëindiging

12.1 Deze Verwerkersovereenkomst treedt in werking op de datum van ondertekening en eindigt van rechtswege bij beëindiging van de Overeenkomst. Verplichtingen met een duurkarakter blijven tussen partijen in stand, zoals de geheimhoudingsverplichting uit artikel 4 van de Verwerkersovereenkomst.

12.2 VERWERKER zal bij beëindiging van de Overeenkomst op verzoek van VERANTWOORDELIJKE en tegen vergoeding van de redelijke kosten de Persoonsgegevens in een gangbaar formaat ter beschikking stellen aan VERANTWOORDELIJKE of aan een door VERANTWOORDELIJKE aangewezen Derde.

12.3 VERWERKER zal na overdracht van de Persoonsgegevens aan VERANTWOORDELIJKE de nog aanwezige Persoonsgegevens vernietigen, tenzij een langere opslag wettelijk verplicht is. VERWERKER zal tevens zorgdragen voor vernietiging van de Persoonsgegevens bij de Sub-verwerkers.

## Artikel 13. Wijziging Verwerkersovereenkomst

13.1 Bij wijzigingen in de Diensten, regelgeving of andere relevante omstandigheden die van invloed zijn op de verwerking van de Persoonsgegevens, zullen Partijen in overleg treden over een eventueel benodigde wijziging van de Verwerkersovereenkomst. De wijzigingen in de tekst van deze Verwerkersovereenkomst kunnen uitsluitend schriftelijk door de bevoegde vertegenwoordigers van Partijen worden overeengekomen.

13.2 Wijzigingen in de Bijlagen kunnen door Partijen op ieder moment schriftelijk worden gedaan onder vermelding van het versienummer en de datum van ingang van de nieuwe versie.

## Artikel 14. Toepasselijk recht / Bevoegde rechter

14.1 Op deze Verwerkersovereenkomst is uitsluitend Nederlands recht van toepassing.

14.2 Alle geschillen die ontstaan naar aanleiding van deze Verwerkersovereenkomst worden beslecht op dezelfde wijze als opgenomen in de Overeenkomst.

BIJLAGE 1

**A. Producten en diensten**

Deze verwerkersovereenkomst is van toepassing op alle producten en diensten van VERWERKER waaronder:

**Cloud Services** zoals:
- Cloud Servers
- Cloud Werkplekken
- Cloud Back-up
- Cloud Monitoring

**Colocatie hosting**
**Voice over IP (VoIP)**
**Domeinnaam registratie**
**E-mail hosting**
**Webhosting**
**File Sync oplossingen**
**Systeembeheer, gebruikersondersteuning en reparatie van hardware**
**Mobiele Telefonie**
**Online Software diensten**
**Hardware en Systeemsoftware**

**B. Aard en doel van de verwerking**

De aard van de verwerking is het opslaan van data en beschikbaar stellen voor gebruik aan VERANTWOORDELIJKE, o.a. door middel van de producten en diensten zoals beschreven in artikel A van Bijlage 1

**C. Contactgegevens**

Voor vragen of opmerkingen over de Verwerkersovereenkomst en Bijlagen is de contactpersoon van

VERWERKER:
Mickcom ICT
E-mail: info@mickcom.nl
Telefoon: +31 (0)348 554821

 

## BIJLAGE 2

**Omschrijving van de technische en organisatorische beveiligingsmaatregelen die door de VERWERKER zijn geïmplementeerd**

Zoals opgenomen in artikel 5 worden hieronder de afspraken tussen partijen vastgelegd over de concrete technische en organisatorische beveiligingsmaatregelen. De getroffen maatregelen zijn opgenomen in deze bijlage en worden aangevuld of gewijzigd indien dat nodig is.

VERANTWOORDELIJKE acht genoemde maatregelen passend voor de Verwerking van de Persoonsgegevens.

**A. Maatregelen van verwerker om te zorgen dat uitsluitend bevoegd personeel van VERWERKER toegang heeft tot de Persoonsgegevens:**

Toegang tot persoonsgegevens is beperkt tot medewerkers van VERWERKER waarvoor autorisatie benodigd is voor uitvoering van de werkzaamheden. Medewerkers commiteren zich aan de geheimhoudingsplicht zoals vastgelegd in de arbeidsovereenkomst.

**B. Maatregelen om de Persoonsgegevens te beschermen tegen verlies of wijziging en tegen onbevoegde of onrechtmatige verwerking, toegang of openbaarmaking**:

Opslag, back-up en retentie van de DATA is vastgelegd in de Service Level Agreement tussen VERWERKER en VERANTWOORDELIJKE.

VERWERKER voorziet in beveiligde toegang tot persoonsgegevens van VERANTWOORDELIJKE d.m.v. zgn. encrypted verbindingen en authenticatie.

**C. Maatregelen voor opsporen van zwakke plekken en incidentenbeheer:**

De dienstverlening van VERWERKER voorziet in incidentenbeheer, regulier syteem- en netwerkbeheer en auditing voor alle van toepassing zijnde componenten.

## BIJLAGE 3 “Procedure Meldplicht Datalekken”

Tussen Partijen zijn met betrekking tot de meldplicht datalekken de volgende afspraken gemaakt:

1) VERWERKER registreert alle Beveiligingsincidenten;
2) In geval van een Beveiligingsincident informeert VERWERKER VERANTWOORDELIJKE binnen 2 uur en zal de relevante informatie over het incident melden aan de hand van de hieronder opgenomen vragenlijst;
3) VERANTWOORDELIJKE zal beoordelen of een melding verricht dient te worden bij de AP. VERANTWOORDELIJKE zal daarbij in overleg treden met VERWERKER;
4) Voordat VERANTWOORDELIJKE de melding bij de AP verricht zal VERANTWOORDELIJKE de inhoud van de melding met VERWERKER bespreken;
5) Indien VERANTWOORDELIJKE oordeelt dat tevens betrokkenen geïnformeerd dienen te worden, zal VERANTWOORDELIJKE de inhoud van die informatie met VERWERKER bespreken.

## Vragenlijst Beveiligingsincident – bij de Procedure Meldplicht Datalekken

De contactpersonen bij VERANTWOORDELIJKE voor de meldplicht datalekken zijn:

[A + gegevens]
[B + gegevens]

VERWERKER zal bij een Beveiligingsincident de volgende vragen beantwoorden:

**Geef een omschrijving van het Beveiligingsincident:**

……..
(bijvoorbeeld “gestolen laptop met klantgegevens” of “een hack op systeem [X]” of “inloggegevens verstuurd naar ontvanger Y ipv X”)

**De persoonsgegevens van hoeveel personen zijn getroffen door het Beveiligingsincident?**

……..
(geef een minimum en maximum aantal aan)

**Omschrijf de groep personen waarop de Persoonsgegevens betrekking hebben.**

……..
(bijvoorbeeld sollicitanten of cliënten van VERANTWOORDELIJKE)

**Is er sprake van één van deze specifieke groepen personen (omcirkel het antwoord):**

Ouderen: JA / NEE
Kinderen: JA / NEE
Zieken of mensen met een verstandelijke beperking: JA / NEE

**Datum en tijdstip van het incident:**

……..
(kan een vast tijdstip zijn of een periode, als dit niet bekend is “onbekend” invullen)

**Wanneer is het beveiligingsincident ontdekt?**

……..

**Wat is de aard van de inbreuk? Omcirkel de antwoorden en vul in waar nodig**

Kan een onbevoegde de gegevens lezen: JA / NEE
Kunnen/zijn de gegevens (worden) gekopieerd door een onbevoegde: JA / NEE Kunnen/zijn de (bron)gegevens (worden) gewijzigd (bijv. hack in het systeem): JA / NEE Kunnen/zijn de (bron)gegevens (worden) verwijderd of vernietigd (bijv. ransom ware of brand datacenter): JA / NEE
Zijn de gegevens gestolen: JA / NEE
Overig: ……
(invullen, of als de aard niet bekend is: “onbekend” invullen)

**Om welk type gegevens gaat het? Omcirkel de antwoorden en vul in waar nodig:**

Naam-, adres- en woonplaatsgegevens: JA / NEE
Telefoonnummer: JA / NEE
E-mailadres of andere adres voor elektronische communicatie: JA / NEE
Inloggegevens (gebruikersnaam/wachtwoord, klantnummer of ander identificatienummer): JA / NEE,
zo ja; welke gegevens zijn het: ……(invullen)
Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer): JA / NEE
Burgerservicenummer (BSN) of sofinummer: JA / NEE
Paspoortkopieën of kopieën van andere legitimatiebewijzen: JA / NEE
Geslacht: JA / NEE
Geboortedatum en/of leeftijd: JA / NEE
(Pas)foto: JA / NEE
Geboorteland: JA / NEE
Medische gegevens (waaronder ook medicijnen of medische hulpmiddelen): JA / NEE
Biometrische gegevens (bijv. vingerafdruk, DNA): JA / NEE,
zo ja; welke gegevens zijn het: …… (invullen)
Gegevens over schulden/kredieten: JA / NEE
Inkomensgegevens: JA / NEE
Gegevens over iemands betalingsverkeer: JA / NEE
Gegevens over wettelijke vertegenwoordiging (bewindvoerder/mentor): JA / NEE
Verslavingsgegevens: JA / NEE
School/werkprestaties: JA / NEE
Gegevens over relationele problemen: JA / NEE
Gegevens over (vermoeden van) mishandeling: JA / NEE
Religie: JA / NEE
Strafrechtelijke gegevens (ook bijv. straatverboden): JA / NEE
Politieke overtuiging: JA / NEE
Vakbondslidmaatschap: JA / NEE
Seksuele voorkeur/geaardheid: JA / NEE
Overige gegevens: …… (invullen)

**Welke gevolgen kan de inbreuk hebben voor de getroffen personen? Omcirkel de antwoorden en vul in waar nodig:**

Stigmatisering of uitsluiting: JA / NEE
Schade aan de gezondheid: JA / NEE
Kans op identiteitsfraude: JA / NEE
Kans op financiële schade (bijv. fraude met creditcardgegevens): JA / NEE
Blootstelling aan spam of phishing: JA / NEE
Andere gevolgen, namelijk: …… (invullen)

**Omschrijf welke technische en organisatorische maatregelen zijn getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?**

……..

**Zijn de gelekte persoonsgegevens beveiligd? Omcirkel de antwoorden en vul in waar nodig:**

Zijn de gegevens versleuteld: JA /NEE,
zo ja; welke versleuteling: …… (invullen)
geldt deze versleuteling voor alle persoonsgegevens of voor een deel? Indien voor een deel, voor welk deel: …… (invullen)

Zijn de gegevens gehasht: JA /NEE,
zo ja; op welke wijze: …… (invullen)

Kunnen de gegevens vanaf afstand worden gewist: JA /NEE,
zo ja; is dat gebeurd en wanneer is dat gebeurd: …… (invullen)

Zijn de gegevens op een andere manier onbegrijpelijk of ontoegankelijk gemaakt: JA /NEE,
zo ja; op welke manier: …… (invullen)

**Zijn er Persoonsgegevens van personen in andere EU-landen getroffen door het Beveiligingsincident? Zo ja, welke uit welke landen:**

……..