

Europese aanbesteding Communicatieverbindingen

Bijlage 4 Verwerkersovereenkomst

The logo for Skal BIOCONTROLE is contained within a white arrow-shaped box pointing to the right. The word "Skal" is written in a bold, sans-serif font, with the letter "k" in red and "S" and "a" in dark green. Below "Skal", the word "BIOCONTROLE" is written in a smaller, dark green, all-caps sans-serif font.

Skal
BIOCONTROLE

Verwerkersovereenkomst

tussen:

1. **Stichting Skal**, statutair gevestigd en kantoorhoudende te (8025 BS) Zwolle aan Dr. Klinkertweg 28a, ingeschreven bij de Kamer van Koophandel onder nummer 41181708, hierna te noemen '**Opdrachtgever**' of '**Verantwoordelijke**'; en
2. **[naam bedrijf]**, statutair gevestigd en kantoorhoudende te **([postcode]) [plaats]** aan **[adres]**, ingeschreven bij de Kamer van Koophandel onder nummer **[kvk-nummer]**, hierna te noemen '**Opdrachtnemer**' of '**Verwerker**',

Hierna gezamenlijk te noemen de '**Partijen**' of ieder afzonderlijk als de '**Partij**'.

Overwegende dat:

- a. Partijen op **[datum]** een overeenkomst dan wel een opdrachtverstrekking hebben gesloten dan wel vastgelegd ('**Hoofdovereenkomst**') met kenmerk en/of referentienummer **[kenmerk vermelden]**;
- b. voor zover Opdrachtnemer in het kader van de Hoofdovereenkomst Persoonsgegevens Verwerkt ten behoeve van Opdrachtgever, Opdrachtgever krachtens artikel 4, onderdeel 7 en onderdeel 8 van de AVG kwalificeert als verwerkingsverantwoordelijke voor de Verwerking van persoonsgegevens en Opdrachtnemer als verwerker.
- c. Privacywetgeving, inclusief nationale wetten ter uitvoering van de Algemene Verordening Gegevensbescherming ('de **Verordening**'), vereist dat dergelijke verwerkingen worden geregeld door een overeenkomst of rechtshandeling die de Verwerker bindt aan de Verantwoordelijke en waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, de verplichtingen van de Verwerker in verband met beveiligingsincidenten en datalekken, het soort persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de Verantwoordelijke worden omschreven; en
- d. Partijen de bovenstaande vereisten in de onderhavige verwerkersovereenkomst ('**Verwerkersovereenkomst**') zoals bedoeld in artikel 28 derde lid van de Verordening wensen te regelen, welke overeenkomst een integraal onderdeel is van de Hoofdovereenkomst.

Partijen verklaren te zijn overeengekomen als volgt:

1. Definities en interpretatie

- 1.1. '**Inbreuk in verband met persoonsgegevens**' '**Persoonsgegevens**', '**Verantwoordelijke**', '**Verwerking**' en '**Verwerker**' hebben de betekenis zoals bedoeld in

de Privacywetgeving. Daarnaast hebben de volgende woorden en zinsdelen de volgende betekenis:

Betrokkene: degene op wie een Persoonsgegeven betrekking heeft;

Privacywetgeving de verordening (EU) 2016/679 ('**Algemene Verordening Gegevensbescherming**') en elke wetgeving of verordening die deze verordening van tijd tot tijd wijzigt of aanvult;

- 1.2. Deze Verwerkersovereenkomst en de Bijlagen vormen een integraal onderdeel van de Hoofdovereenkomst. en een verwijzing naar de Verwerkersovereenkomst is inclusief een verwijzing naar de Bijlagen.
- 1.3. In geval van inconsistentie tussen de bepalingen van deze Verwerkersovereenkomst en de Hoofdovereenkomst, gelden de bepalingen van deze Verwerkersovereenkomst.
- 1.4. In geval van nietigheid c.q. vernietigbaarheid van een of meer bepalingen uit deze Verwerkersovereenkomst blijven de overige bepalingen onverkort van kracht.

2. Voorwerp van deze overeenkomst

- 2.1. Deze Verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Opdrachtnemer in het kader van de Hoofdovereenkomst.
- 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. Opdrachtnemer garandeert de toepassing van passende technische en organisatorische maatregelen, opdat de Verwerking aan de vereisten van de Privacywetgeving voldoet en de bescherming van de rechten van de Betrokkene is gewaarborgd.
- 2.4. Opdrachtnemer garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

3. Inwerkingtreding en duur

- 3.1. Deze Verwerkersovereenkomst treedt in werking op het moment waarop deze door Partijen is ondertekend.
- 3.2. Deze Verwerkersovereenkomst zal van kracht zijn gedurende de looptijd van de Hoofdovereenkomst. Indien de Hoofdovereenkomst eindigt, eindigt deze Verwerkersovereenkomst van rechtswege.
- 3.3. Geen van Partijen kan deze Verwerkersovereenkomst tussentijds opzeggen.

- 3.4. De bepalingen uit deze Verwerkersovereenkomst die de strekking hebben om na beëindiging van deze overeenkomst hun gelding te behouden, waaronder begrepen maar niet beperkt tot de artikelen 6 (geheimhouding), 10.2 (terugbezorgen of wissen Persoonsgegevens), 12 (vrijwaring en boete) en dit artikellid blijven na het eindigen van de Verwerkersovereenkomst onverminderd van kracht.

4. Omvang verwerkingsbevoegdheid Opdrachtnemer

- 4.1. Opdrachtnemer Verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van voorafgaande schriftelijke instructies van Opdrachtgever behoudens afwijkende wettelijke voorschriften die op Opdrachtnemer van toepassing zijn.
- 4.2. Indien een instructie als bedoeld in het eerste lid naar het oordeel van Opdrachtnemer in strijd is met een wettelijk voorschrift inzake gegevensbescherming, stelt hij Opdrachtgever daarvan voorafgaand aan de Verwerking schriftelijk in kennis, tenzij een wettelijk voorschrift deze kennisgeving verbiedt.
- 4.3. Het is Opdrachtnemer niet toegestaan Persoonsgegevens waarvoor Opdrachtgever Verantwoordelijke is aan anderen dan Opdrachtgever te verstrekken, tenzij op schriftelijk verzoek van Opdrachtgever, of met diens voorafgaande schriftelijke toestemming.
- 4.4. Indien Opdrachtnemer op grond van een wettelijk voorschrift Persoonsgegevens waarvoor Opdrachtgever Verantwoordelijk is aan anderen dan Opdrachtgever dient te verstrekken, informeert hij Opdrachtgever onmiddellijk, en zo mogelijk voorafgaand aan de verstrekking.
- 4.5. Opdrachtnemer heeft geen zeggenschap over het doel van en de middelen voor de Verwerking van Persoonsgegevens.
- 4.6. Opdrachtnemer geeft Opdrachtgever op eerste verzoek inzage in het register van verwerkingsactiviteiten zoals bedoeld in artikel 30 lid 2 AVG met betrekking tot de Persoonsgegevens waarop deze Verwerkersovereenkomst betrekking heeft.

5. Beveiliging

- 5.1. In aanvulling op de Hoofdovereenkomst en onverminderd het in artikel 2.3 bepaalde, treft Opdrachtnemer de technische en organisatorische beveiligingsmaatregelen zoals beschreven in **Bijlage 2**. [dit moet afgestemd worden met de Verwerker]
- 5.2. Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Opdrachtnemer waarborgt een op het risico afgestemd beveiligingsniveau.

- 5.3. Indien en voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal Opdrachtnemer aanvullende maatregelen treffen met het oog op de beveiliging van de Persoonsgegevens.
- 5.4. Opdrachtnemer Verwerkt Persoonsgegevens niet buiten de Europese Unie, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Opdrachtgever en behoudens afwijkende wettelijke verplichtingen.
- 5.5. Opdrachtnemer informeert Opdrachtgever onmiddellijk zodra hij onrechtmatige Verwerkingen van Persoonsgegevens of inbreuken op beveiligingsmaatregelen zoals genoemd in het eerste en tweede lid signaleert en alle en alle redelijkerwijs benodigde maatregelen treffen om deze en verdere onrechtmatige Verwerkingen of inbreuken te beëindigen, te voorkomen of te beperken. Een eventuele verplichting van Opdrachtnemer om de door Opdrachtgever daardoor geleden schade te vergoeden, blijft onverminderd bestaan.
- 5.6. Opdrachtnemer verleent Opdrachtgever bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de Verordening.

6. Geheimhouding door personeel van Opdrachtnemer

- 6.1. Opdrachtnemer zorgt ervoor dat het personeel dat bevoegd is om de Persoonsgegevens te verwerken zich tot vertrouwelijkheid verbindt gedurende en na hun dienstverband (bijvoorbeeld door middel van een geheimhoudingsovereenkomst), voor zover het niet reeds tot een wettelijke verplichting tot geheimhouding is gehouden.
- 6.2. Opdrachtnemer toont op verzoek van Opdrachtgever aan dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 6.1.

7. Subverwerker

- 7.1. Opdrachtnemer schakelt bij de Verwerking geen andere verwerker (**Subverwerker**) in zonder voorafgaande schriftelijke toestemming van Opdrachtgever.
- 7.2. Indien Opdrachtnemer na daartoe verkregen toestemming van Opdrachtgever een Subverwerker inschakelt om ten behoeve van Opdrachtgever verwerkingsactiviteiten te verrichten, worden aan deze Subverwerker bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in deze Verwerkersovereenkomst zijn opgenomen.
- 7.3. Opdrachtnemer blijft volledig aansprakelijk voor de nakoming van zijn verplichtingen uit hoofde van deze Verwerkersovereenkomst, met inbegrip van de door de Subverwerker verwerkte Persoonsgegevens.

8. Samenwerking en Betrokkenen

- 8.1. Opdrachtnemer verleent Opdrachtgever volledige medewerking om binnen de wettelijke termijnen te voldoen aan diens plicht om verzoeken om uitoefening van de in hoofdstuk III van de Verordening vastgelegde rechten van de Betrokkene te beantwoorden, zoals, maar niet beperkt tot, verzoeken met betrekking tot de rechten op inzage, rectificatie, vergetelheid en dataportabiliteit. Tenzij Opdrachtgever anders bepaalt, verloopt de communicatie met de Betrokkene via Opdrachtgever en niet tussen Opdrachtnemer en de Betrokkene onderling.
- 8.2. Opdrachtnemer verleent Opdrachtgever op eerste verzoek bijstand bij het doen nakomen van de op Opdrachtgever rustende verplichtingen op grond van de Privacywetgeving betreffende de Verwerking van Persoonsgegevens, zoals met betrekking tot - maar niet beperkt tot - het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) en een eventuele daaruit voortkomende verplichte voorafgaande raadpleging van de Autoriteit Persoonsgegevens en het voldoen aan verzoeken van de Autoriteit Persoonsgegevens of een andere overheidsinstantie.

9. Inbreuk in verband met Persoonsgegevens

- 9.1. Opdrachtnemer informeert Opdrachtgever onmiddellijk, zodra hij kennis heeft genomen van een Inbreuk in verband met Persoonsgegevens, overeenkomstig de afspraken zoals vastgelegd in **Bijlage 3**.
- 9.2. Opdrachtnemer informeert Opdrachtgever 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.

10. Bewaartermijnen en terugbezorgen of wissen Persoonsgegevens

- 10.1. De Verantwoordelijke zal Verwerker adequaat informeren over (wettelijke) bewaartermijnen die van toepassing zijn op de verwerking van Persoonsgegevens door de Verwerker. De Verwerker zal de Persoonsgegevens niet langer verwerken dan overeenkomstig deze bewaartermijnen.
- 10.2. Na afloop van deze Verwerkersovereenkomst draagt Opdrachtnemer, naar gelang de keuze van Opdrachtgever, zorg voor het terugbezorgen aan Opdrachtgever of het wissen van alle Persoonsgegevens. Opdrachtnemer verwijdert kopieën, behoudens afwijkende wettelijke voorschriften.

11. Informatieverplichting en audit

- 11.1. Opdrachtnemer stelt alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst zijn en worden nagekomen.
- 11.2. Opdrachtnemer verleent alle benodigde medewerking aan audits. Opdrachtnemer voert de door Opdrachtgever aangegeven aanbevelingen ter verbetering uit binnen de daartoe door Opdrachtgever te bepalen termijn. Bij de bepaling van de termijn wordt rekening gehouden met het belang van de verbetering en de daarvoor redelijkerwijs benodigde uitvoeringstijd.

12. Vrijwaring en Boete

- 12.1. Opdrachtnemer vrijwaart Opdrachtgever tegen alle vorderingen en andere aanspraken van derden en de daaruit voortvloeiende schade als gevolg van een schending van deze Verwerkersovereenkomst door Opdrachtnemer of enig ander handelen of nalaten van Opdrachtnemer. Te denken valt hierbij aan een tekortkoming door Opdrachtnemer en/of diens Subverwerkers en/of enige schending door Opdrachtnemer en/of diens Subverwerkers van de Privacywetgeving. Opdrachtnemer draagt zorg voor afdoende dekking van de aansprakelijkheid.
- 12.2. De in de Hoofdovereenkomst mogelijk opgenomen beperkingen van aansprakelijkheid zijn niet van toepassing.
- 12.3. In geval van overtreding van een van de bepalingen van deze Verwerkersovereenkomst verbeurt Opdrachtnemer, ongeacht of de overtreding aan Opdrachtnemer kan worden toegerekend en zonder voorafgaande ingebrekestelling of gerechtelijke procedure, ten behoeve van Opdrachtgever een onmiddellijk opeisbare boete van EUR 10.000,- per overtreding en daarnaast een boete van EUR 1.000,- voor elke dag dat die overtreding voortduurt, zonder dat sprake hoeft te zijn van enige vorm van schade en onverminderd de overige rechten van Opdrachtgever, waaronder haar recht om naast de boete schadevergoeding te vorderen.

13. Toepasselijk recht en bevoegde rechter

- 13.1. Op deze Verwerkersovereenkomst is Nederlands recht van toepassing. Alle geschillen die voortvloeien uit deze overeenkomst zullen exclusief worden voorgelegd aan de in de Hoofdovereenkomst aangewezen rechtbank of arbiter(s).
- 13.2. Alle bijgevoegde bijlagen maken een onlosmakelijk onderdeel uit van deze overeenkomst en kunnen in onderling overleg met uitdrukkelijke schriftelijke instemming van de Opdrachtgever worden gewijzigd.

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

Opdrachtgever	Opdrachtnemer
Handtekening:	Handtekening:
Organisatie: Stichting Skal	Organisatie: [naam invullen]
Naam: de heer/mevrouw [naam invullen]	Naam: de heer/mevrouw [naam invullen]
Titel/functie: [invullen]	Titel/functie: [invullen]
Datum: [invullen]	Datum: [invullen]
Plaats: Zwolle	Plaats: [invullen]

Bijlage 1. De Verwerking van Persoonsgegevens

In deze bijlage moet in ieder geval het volgende worden gespecificeerd:

Het onderwerp/aard en doel van de Verwerking	
Het soort Persoonsgegevens	
Beschrijving categorieën Persoonsgegevens	
Beschrijving categorieën Betrokkenen	
Beschrijving categorieën ontvangers van Persoonsgegevens	

Voor de inhoud van deze bijlage kan onder meer gebruik worden gemaakt van de registratie die de Verwerkingsverantwoordelijke op grond van artikel 30 van de Verordening dient aan te houden.

BIJLAGE 2. Passende technische en organisatorische maatregelen

Opdrachtnemer heeft een (informatie)beveiligingsbeleid opgesteld en de hierin beschreven maatregelen aantoonbaar geïmplementeerd. Dit beleid wordt met regelmaat getoetst en geactualiseerd. De beveiligingsmaatregelen zijn passend voor en in overeenstemming met de waarde van de te verwerken gegevens.

Wanneer Opdrachtnemer gebruik maakt van subverwerkers, dienen deze expliciet te zijn beschreven en bekend te zijn bij Opdrachtgever. De subverwerker houdt zich aan minimaal dezelfde beveiligingseisen en -maatregelen als Opdrachtnemer.

Organisatie van informatiebeveiliging

Verantwoordelijkheden ten aanzien van het beschermen van Persoonsgegevens zijn binnen de organisatie Opdrachtnemer expliciet benoemd en belegd.

Personele maatregelen

Verwerker heeft aantoonbaar bevoegd en bekwaam personeel. Zowel bevoegd en bekwaam voor het verwerken van de gegevens als voor het beveiligen en beschermen van de gegevens.

De personeelsleden zijn via een schriftelijke overeenkomst verplicht tot geheimhouding van alle informatie van Opdrachtgever.

Toegang tot Persoonsgegevens

Toegang tot Persoonsgegevens is beperkt op basis van het need-to-know principe. Alleen wanneer toegang tot Persoonsgegevens daadwerkelijk benodigd is voor het uitvoeren van de werkzaamheden wordt deze toegang ook ingeregeld. Zodra bevoegdheden van personen veranderen, wordt de toegang tot gegevens hierop aangepast.

Verwerking op mobiele apparatuur

Wanneer Persoonsgegevens worden verwerkt op mobiele apparatuur, waaronder tablets, laptops en/of smartphones, dan dienen deze apparaten versleuteld (encrypted) te zijn conform marktstandaarden.

Fysieke beveiliging

Opdrachtnemer zorgt ervoor dat Persoonsgegevens worden verwerkt in een fysiek beveiligde omgeving, met passende bescherming tegen dreigingen van buitenaf.

IT-technische maatregelen

Opdrachtnemer neemt passende maatregelen om de IT-omgeving te beveiligen. Informatiesystemen, componenten en middelen zijn actueel en worden door de fabrikant officieel ondersteund.

Alle software wordt op basis van een gestructureerd proces voorzien van de laatste patches en updates. Waar technisch mogelijk wordt gebruik gemaakt van antivirussoftware.

Netwerken en informatiesystemen worden passend afgeschermd op basis van fysieke of logische scheiding, waarbij wordt gewaarborgd dat informatie van Opdrachtgever niet vermengd kan worden met dat van andere klanten van Opdrachtnemer.

Wanneer informatie over openbare netwerken of anderszins publiek beschikbaar kan komen, worden cryptografische maatregelen genomen om de informatie te beschermen tegen onbevoegde inzage.

Periodiek worden vulnerability scans en penetratietests uitgevoerd voor het toetsen van de beveiliging.

Toegang op afstand

Wanneer medewerkers van Opdrachtnemer toegang op afstand (bijvoorbeeld telewerken via internet) kunnen krijgen tot Persoonsgegevens, is deze toegang afgeschermd met een versleutelde verbinding. Toegang op afstand kan alleen worden verkregen door middel van het toepassen van 2 factor authenticatie.

Beheer van incidenten

Opdrachtnemer verplicht zijn medewerkers incidenten met betrekking tot informatiebeveiliging en privacy zo snel mogelijk te melden en deze op basis van de ernst op te volgen. Enkele voorbeelden van incidenten zijn:

- Uitval van dienstverlening, apparatuur of voorzieningen;
- Systeemstoringen of -overbelasting;
- Menselijke fouten;
- Niet-naleven van beleid en/of richtlijnen;
- Inbreuk op fysieke beveiligingsmaatregelen;
- Ongecontroleerde systeemwijzigingen;
- Storingen aan software of hardware;
- Virusuitbraak;
- Toegangsovertredingen (digitaal of fysiek).
- datalek

Alle medewerkers, tijdelijke medewerkers, onderaannemers en derde partijen die op enigerlei wijze gebruik maken van informatie of informatiesystemen van Opdrachtnemer zijn verplicht om (mogelijke) lekken en inbreuken in de informatiebeveiliging te melden als incident. Hiertoe wordt aan deze betrokkenen het incidentmeldingsproces van Opdrachtnemer kenbaar gemaakt.

Opdrachtnemer monitort toegang tot Persoonsgegevens en het mogelijk lekken hiervan.

Continuïteit van de dienstverlening

Opdrachtnemer neemt binnen de dienstverlening passende technische en organisatorische maatregelen om continuïteit te waarborgen. Wanneer de overeenkomst tussen Opdrachtgever en Opdrachtnemer eindigt, verplicht Opdrachtnemer zich te zorgen dat de dienstverlening van Opdrachtgever gewaarborgd blijft in de transitie naar de nieuwe leverancier van Opdrachtgever.

Overige maatregelen

De maatregelen beschreven in deze bijlage pretenderen niet concreet of volledig te zijn. Opdrachtgever verwacht dat Opdrachtnemer zich actief opstelt bij het beschermen van Persoonsgegevens en het nemen van maatregelen om deze te beschermen. In wederzijds overleg kunnen verbeteringen ten aanzien van de Verwerkersovereenkomst en de beschreven maatregelen worden besproken.

BIJLAGE 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens

In deze bijlage moeten de afspraken over hoe Opdrachtnemer Opdrachtgever over Inbreuken in verband met Persoonsgegevens gaat informeren worden gespecificeerd.

Er is sprake van een datalek als er een inbreuk in verband met persoonsgegevens heeft plaatsgevonden.

Alleen een dreiging of een tekortkoming in de beveiliging is niet voldoende; er moeten daadwerkelijk persoonsgegevens gelekt zijn.

Onder een datalek verstaat de Autoriteit Persoonsgegevens persoonsgegevens die gelekt of vernietigd zijn als gevolg van een beveiligingsincident. Bij het lek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking. Bij verlies zijn de persoonsgegevens er niet meer.

Onder onrechtmatige verwerking vallen bijvoorbeeld onbevoegde kennisneming, wijziging, aantasting of de verstrekking daarvan.

Voorbeelden van inbreuken in verband met persoonsgegevens kunnen zijn:

- kwijtraken van een USB -stick
- diefstal van een laptop
- inbraak door een hacker
- persoonsgegevens per ongeluk gepubliceerd
- hacking, malware of fishing
- persoonsgegevens aan verkeerde persoon verstuurd
- calamiteiten zoals brand in een datacentrum.

In deze Procedure Datalek wordt in meer detail uiteengezet hoe Opdrachtnemer in onverhoopt geval met het verlies van dergelijke persoonsgegevens omgaat.

Uitgangspunten

1. De Opdrachtnemer verwerkt persoonsgegevens overeenkomstig de instructies en uiteindelijke verantwoordelijkheid van de Opdrachtgever.
2. De Opdrachtnemer neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens, zoals tevens staat beschreven in de tussen Opdrachtgever en Opdrachtnemer overeengekomen hoofdovereenkomst;

Direct melding doen bij de FG Opdrachtgever

3. De data lek melding moet Opdrachtnemer direct via email en telefonisch worden gedaan bij de Functionaris gegevensbeschermmer van de Opdrachtgever (kortweg FG) en schriftelijk worden vastgelegd.
4. Het telefoonnummer van de FG luidt 038 – 42 681 65

5. Het e-mail adres van de FG luidt jurist@skal.nl
6. De FG meldt het datalek zo nodig bij de Autoriteit Persoonsgegevens.
7. De FG krijgt van de Opdrachtnemer de volgende gegevens en legt deze gegevens ook vast:
 - naam van de melder;
 - de contactpersoon voor de melding;
 - datum en tijd van de melding;
 - aard van de inbreuk en risico op verlies of onrechtmatig gebruik gegevens;
 - welke persoonsgegevens vallen onder de melding;
 - om welk aantal gegevensrecords gaat het;
 - welke (groepen) personen zijn betrokken bij de melding;
 - welke maatregelen zijn of worden door de melder getroffen;
 - welke gevolgen zijn er volgens de melder voor de betrokkenen.

Escalatie bij afwezigheid

8. Bij afwezigheid van de FG wordt diens rol ingevuld door een waarnemer van Opdrachtgever. Buiten kantoor tijden en in het weekend wordt de melding door de Opdrachtnemer gedaan via jurist@skal.nl.
9. Opdrachtnemer is ervan op de hoogte dat een datalek door Opdrachtgever zo spoedig mogelijk, maar uiterlijk binnen 72 uur, gemeld moet worden bij de Autoriteit Persoonsgegevens.

Melding

10. Met het oog daarop zal Opdrachtnemer al het mogelijke doen om Opdrachtgever in staat te stellen deze melding tijdig en volledig te doen. Opdrachtnemer neemt in het geval van een datalek of **een vermoeden daarvan** zo spoedig contact op met de FG of diens plaatsvervanger van Opdrachtgever, ook indien nog niet alle relevante informatie bekend is.
11. Opdrachtnemer zal Opdrachtgever binnen 48 uur na constatering van het datalek voorzien van de benodigde gegevens voor het doen van de melding, zoals omschreven op het formulier bij het Meldloket Datalekken.
12. Indien binnen deze termijn de benodigde gegevens nog niet beschikbaar zijn, zal Opdrachtnemer binnen deze termijn de beschikbare gegevens aan Opdrachtgever aanleveren, met een inschatting van de termijn waarop de overige gegevens beschikbaar zullen komen of de reden waarom deze gegevens niet kunnen worden aangeleverd.
13. Opdrachtnemer zal Opdrachtgever voortdurend op de hoogte houden van actuele ontwikkelingen rondom het datalek en van de maatregelen die Opdrachtnemer treft om de gevolgen van het incident te beperken en herhaling te voorkomen.
14. Opdrachtgever zal Opdrachtnemer op de hoogte houden van wijzigingen in de contactpersonen die aanspreekpunt zijn in het geval van een (mogelijk) datalek.

Communicatie

15. Alle communicatie zowel intern als extern over het datalek verloopt via de Opdrachtgever;

16. De Opdrachtgever stelt vast of de pers dan wel andere derden geïnformeerd moet worden;

Informatie die ten minste door Opdrachtnemer moet worden verstrekt

Aard van de Inbreuk in verband met Persoonsgegevens , waaronder betrokken categorie en aantal betrokkenen
De Persoonsgegevens en Betrokkene
Waarschijnlijke gevolgen van de Inbreuk in verband met Persoonsgegevens
Maatregelen die Opdrachtnemer heeft voorgesteld of genomen om de Inbreuk in verband met Persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan

Einde document.