Instructie bij Model Verwerkersovereenkomst

SURF Juridisch Normenkader (Cloud)services, Bijlage B

(concept versie)

Utrecht, april 2019
Versienummer: 3.0

Colofon

Instructie bij Model Verwerkersovereenkomst

SURF
Postbus 19035
NL-3501 DA Utrecht
T +31 88 787 30 00

info@surf.nl
www.surf.nl

April 2019

SURF is de ICT-samenwerkingsorganisatie van het Nederlandse hoger onderwijs en onderzoek.

Inleiding

Dit is een instructie en uitleg die hoort bij de Model Verwerkersovereenkomst, versie 3.0 (april 2019) welke onderdeel is van het SURF Juridisch Normenkader (Cloud)services.

Een verwerkersovereenkomst is specifiek gericht op de verwerking van persoonsgegevens. In deze overeenkomst staan dus enkel bepalingen over persoonsgegevens.

Onderwerpen die breder zijn dan dit, worden doorgaans opgenomen in de hoofdovereenkomst. Denk daarbij bijvoorbeeld aan intellectueel eigendom (dat kan ook gaan om data die geen persoonsgegevens zijn). Standaardbepalingen om deze onderwerpen in de hoofdovereenkomst te regelen zijn te vinden in de notitie van het SURF Juridisch Normenkader (Cloud)services.

Dit document zal verder worden ontwikkeld en er zullen regelmatig updates verschijnen om beter aan te sluiten bij vragen die er vanuit de doelgroep zijn. Het document biedt houvast bij het gebruik van de verwerkersovereenkomst, maar raadpleeg bij vragen en onduidelijkheden altijd een (juridisch) adviseur binnen uw organisatie.

LEESWIJZER

In dit document wordt, door middel van kaders zoals deze, bij bepaalde bepalingen een uitleg gegeven waarom de bepalingen van belang is en hoe deze gelezen moet worden. Ook wordt verwezen naar wet- en regelgeving waarop de bepaling is gebaseerd of waar de bepaling een uitwerking op is. Daarnaast bevat dit document een instructie die helpt bij het invullen van Bijlage A.

Er wordt in het document verwezen naar de volgende wetgeving, regelgeving, documentatie en websites:

De Algemene Verordening Gegevensbescherming (AVG)
De AVG is een Europese verordening die rechtstreeks van toepassing is in alle EU-lidstaten sinds 25 mei 2018.

Nederlandse Uitvoeringswet Algemene verordening Gegevensbescherming (Uitvoeringswet)
Deze wet vormt de uitvoering van de AVG in Nederland.

Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming
Op 22 januari 2018 heeft het Ministerie van Justitie en Veiligheid een handleiding gepubliceerd waarin de belangrijkste bepalingen uit de AVG en de Uitvoeringswet worden toegelicht. De Handleiding is te vinden via de volgende link:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleidingalgemeneverordeninggegevensbescherming.pdf.

GÉANT Data Protection Code of Conduct
Een door GÉANT ontwikkelde Europese gedragscode, die Service Providers eenzijdig kunnen ondertekenen, om zo aan te geven dat zij voldoen aan de strenge Europese beveiliging- en privacywetgeving: https://geant3plus.archive.geant.net/uri/dataprotection-code-of-conduct/V1/Documents/GEANT_DP_CoC_ver1.0.pdf.

Guidelines meldplicht datalekken
Guidelines voor het melden van datalekken, gepubliceerd door de Artikel 29 Werkgroep en te vinden op de website van de Autoriteit Persoonsgegevens:
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken.

De website van de Autoriteit Persoonsgegevens
Verwijzingen naar nieuwsberichten en uitleg van wetgeving.

Handreiking Beveiligingsmaatregelen, Bijlage C Juridisch Normenkader
Handreiking over de invulling van een passend beveiligingsniveau, horend bij het SURF Juridisch Normenkader (Cloud)services. Versie april 2018. Het document is te vinden op de website van SURF: https://www.surf.nl/binaries/content/assets/surf/nl/2018/jnk-2018/surf_c-handreiking-beveiligingsmaatregelen---bijlage-c---versie-mei-2018.pdf.

Handreiking Auditverplichting, Bijlage D Juridisch Normenkader
Leidraad voor de invulling van de auditverplichting uit de verwerkersovereenkomst, horend bij het SURF Juridisch Normenkader (Cloud)services. Versie maart 2018. Het document is te vinden op de website van SURF:
https://www.surf.nl/binaries/content/assets/surf/nl/2018/jnk-2018/surf_d-handreiking-auditverplichting---bijlage-d---versie-mei-2018.pdf.

DE ONDERGETEKENDEN:

<NAAM INSTELLING>, gevestigd aan <ADRES> te <PLAATS>, Kamer van Koophandel nummer <KVK> en rechtsgeldig vertegenwoordigd door **<VERTEGENWOORDIGER>** (hierna: "**Verwerkingsverantwoordelijke**");

en

<NAAM LEVERANCIER>, gevestigd aan <ADRES> te <PLAATS>, Kamer van Koophandel nummer <KVK> en rechtsgeldig vertegenwoordigd door **<VERTEGENWOORDIGER>** (hierna: "**Verwerker**");

Hierna gezamenlijk te noemen: "**Partijen**" en individueel te noemen "**Partij**";

NEMEN HET VOLGENDE IN AANMERKING:

- Partijen hebben op <DATUM……> een overeenkomst gesloten met kenmerk <KENMERK VAN DE OVEREENKOMST……> met betrekking tot <ONDERWERP VAN DE OVEREENKOMST……>. Ter uitvoering van de Overeenkomst verwerkt Verwerker ten behoeve van Verwerkingsverantwoordelijke Persoonsgegevens;

  In het kader van de verwerkersovereenkomst wordt expliciet bepaald dat, voor zover de leverancier persoonsgegevens verwerkt voor de instelling, de instelling de verwerkingsverantwoordelijke is en de leverancier de verwerker in de zin van de AVG. Door dit expliciet te benoemen is duidelijk welke rechten en plichten van de AVG van toepassing zijn op de instelling en de leverancier.

  In de AVG wordt als 'verwerkingsverantwoordelijke' aangemerkt de natuurlijke- of rechtspersoon die het doel ('waarom') en de middelen ('hoe') van de verwerking bepaalt. Als 'verwerker' wordt aangemerkt de natuurlijke- of rechtspersoon die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

  Wet- en regelgeving:
  - Artikel 4 lid 7 en lid 8 AVG

- In het kader van het uitvoeren van de Overeenkomst is <NAAM LEVERANCIER> aan te merken als Verwerker in de zin van de AVG en is <NAAM INSTELLING> aan te merken als Verwerkingsverantwoordelijke in de zin van de AVG;

- Partijen wensen zorgvuldig en in overeenstemming met de AVG en andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens om te gaan met de Persoonsgegevens die ter uitvoering van de Overeenkomst verwerkt (zullen) worden;
- Partijen wensen in overeenstemming met de AVG en andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens hun rechten en plichten ten aanzien van de Verwerking van Persoonsgegevens van Betrokkenen Schriftelijk vast te leggen in deze Verwerkersovereenkomst.

Partijen zijn verplicht de verwerking van persoonsgegevens door verwerker vast te leggen in een overeenkomst of andere rechtshandeling.

Wet- en regelgeving:
- Artikel 28 lid 3 AVG

EN ZIJN ALS VOLGT OVEREENGEKOMEN:

ARTIKEL 1. DEFINITIES

In deze Verwerkersovereenkomst hebben de met hoofdletter geschreven begrippen de in dit artikel opgenomen betekenis. Waar de definitie in dit artikel in het enkelvoud is opgenomen, wordt ook het meervoud daaronder begrepen en vice versa, tenzij uitdrukkelijk anders vermeld of uit de context anders blijkt. Indien een met hoofdletter geschreven begrip niet in dit artikel is opgenomen wordt aan dit begrip de betekenis van de definitie uit artikel 4 AVG toegekend.

1.1 AVG: de 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 Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

1.2 Bijlage: een bijlage bij deze Verwerkersovereenkomst, die een integraal onderdeel vormt van deze Verwerkersovereenkomst.

1.3 Dienst: de op grond van de Overeenkomst te leveren dienst(en) door Verwerker aan Verwerkingsverantwoordelijke.

1.4 DPIA: de gegevensbeschermingseffectbeoordeling die vóór de Verwerking ten aanzien van het effect van de beoogde verwerkingsactiviteiten op de bescherming van Persoonsgegevens wordt uitgevoerd, zoals bedoeld in artikel 35 AVG.

1.5 Medewerker: de door Verwerker ingeschakelde werknemers en andere personen, niet zijnde Sub-verwerkers, waarvan de werkzaamheden onder zijn verantwoordelijkheid vallen en die worden ingeschakeld door Verwerker ter uitvoering van de Overeenkomst.

1.6 Overeenkomst: de overeenkomst die tussen Verwerkingsverantwoordelijke en Verwerker is gesloten en op grond waarvan Verwerker Persoonsgegevens ten behoeve van de uitvoering van deze overeenkomst voor Verwerkingsverantwoordelijke verwerkt.

1.7 Schriftelijk: op schrift gesteld of langs de elektronische weg, zoals bedoeld in artikel 6:227a van het Burgerlijk Wetboek.

1.8 Sub-verwerker: een andere verwerker, waaronder maar niet beperkt tot groepsmaatschappijen, zustermaatschappijen, dochtermaatschappijen en hulpleveranciers, die Verwerker inschakelt ter ondersteuning van de uitvoering van de Overeenkomst.

1.9 Verwerkersovereenkomst: de onderhavige overeenkomst inclusief Bijlagen, zoals bedoeld in artikel 28 lid 3 AVG.

ARTIKEL 2. VOORWERP VAN DE VERWERKERSOVEREENKOMST

2.1 De Verwerkersovereenkomst vormt een aanvulling op de Overeenkomst en vervangt eventuele eerder gemaakte afspraken tussen Partijen ten aanzien van de Verwerking van Persoonsgegevens. Bij tegenstrijdigheid tussen de bepalingen uit de Verwerkersovereenkomst en de Overeenkomst, prevaleren de bepalingen uit de Verwerkersovereenkomst.

Het kan zijn dat er in de hoofdovereenkomst of algemene voorwaarden ook afspraken zijn gemaakt omtrent privacy. Het is verstandig om deze hoofdovereenkomst inhoudelijk af te stemmen op de verwerkersovereenkomst om tegenspraak te voorkomen. Aangezien het toch kan gebeuren dat er tegenstrijdigheden in beide overeenkomsten staan, is in artikel 2 lid 1 opgenomen dat de verwerkersovereenkomst voor de hoofdovereenkomst gaat. Het is belangrijk dat er in de hoofdovereenkomst geen tegenstrijdige rangorde staat.

2.2 De bepalingen uit de Verwerkersovereenkomst gelden voor alle Verwerkingen die plaatsvinden ter uitvoering van de Overeenkomst. Verwerker brengt Verwerkingsverantwoordelijke onverwijld op de hoogte indien Verwerker reden heeft om aan te nemen dat Verwerker niet langer aan de Verwerkersovereenkomst kan voldoen.

Alle bepalingen uit de verwerkersovereenkomst zijn enkel van toepassing op verwerkingen van persoonsgegevens in het kader van de dienst.

De instelling mag als verwerkingsverantwoordelijke enkel een beroep doen op leveranciers die afdoende garanties bieden met betrekking tot het nakomen van de vereisten uit de AVG en de bescherming van de rechten van betrokkenen. Het is daarom belangrijk dat de leverancier de instelling direct op de hoogte stelt als er enige reden is om te twijfelen aan de mogelijkheid voor de leverancier om de verwerkersovereenkomst na te komen.

Wet- en regelgeving:

- Artikel 28 lid 1 AVG

2.3 Verwerkingsverantwoordelijke geeft Verwerker opdracht en instructies om de Persoonsgegevens te verwerken namens de Verwerkingsverantwoordelijke.

2.3.1 De instructies van Verwerkingsverantwoordelijke zijn nader omschreven in de Verwerkersovereenkomst en de Overeenkomst. Verwerkingsverantwoordelijke kan naar redelijkheid Schriftelijk aanvullende of afwijkende instructies geven.

2.3.2 Partijen leggen in Bijlage A vast welke Verwerkingen de Verwerker in opdracht van de Verwerkingsverantwoordelijke uitvoert. Verwerker is uitsluitend tot de in Bijlage A gespecificeerde Verwerkingen gerechtigd.

De leverancier mag uitsluitend die verwerkingen verrichten die zijn vastgelegd in deze verwerkersovereenkomst. In bijlage A wordt gespecificeerd om welke verwerkingen het gaat, de doeleinden van de verwerking, de categorieën van persoonsgegevens, de categorieën van betrokkenen, de frequentie van de te verrichten audits en de bewaartermijn van de persoonsgegevens.

Bij de categorieën van persoonsgegevens speelt dataminimalisatie een rol: er worden niet meer persoonsgegevens verwerkt dan voor het aanbieden van de dienst noodzakelijk is.

Wet- en regelgeving:

- Artikel 28 lid 3, aanhef en onder a AVG

2.3.3 Niettegenstaande artikel 8 en 9, verwerkt Verwerker de Persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke en op basis van de instructies van Verwerkingsverantwoordelijke zoals bedoeld in artikel 2.3.1 en 2.3.2. Verwerker verwerkt de Persoonsgegevens uitsluitend voor zover de Verwerking noodzakelijk is ter uitvoering van de Overeenkomst, nimmer ten eigen nutte, ten nutte van Derden en/of voor reclamedoeleinden c.q. andere doeleinden, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot Verwerking verplicht. In dat geval stelt Verwerker Verwerkingsverantwoordelijke voorafgaand aan de Verwerking Schriftelijk op de hoogte van deze bepaling, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

De leverancier mag uitsluitend verwerkingen verrichten op basis van schriftelijke instructies van de instelling. Dit betekent in de praktijk dat de leverancier slechts de persoonsgegevens van de instelling mag verwerken voor zover dat noodzakelijk is om de dienstverlening aan de instelling te leveren. De leverancier mag de persoonsgegevens niet voor eigen doeleinden (zoals reclame) gebruiken. De doeleinden van de verwerking worden door de instelling bepaald en opgenomen in bijlage A van de verwerkersovereenkomst.

Wet- en regelgeving:

- Artikel 28 lid 3 onder a en artikel 29 AVG

2.4 Verwerker en Verwerkingsverantwoordelijke leven de AVG en andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens na. Verwerker stelt de Verwerkingsverantwoordelijke onmiddellijk in kennis indien naar mening van Verwerker een instructie van Verwerkingsverantwoordelijke inbreuk oplevert op de AVG en/of andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

Onder de AVG hebben zowel verwerkingsverantwoordelijken als verwerkers eigen verplichtingen. De leverancier dient op grond van de AVG de instelling direct op de hoogte te stellen als hij van mening is dat een instructie van de instelling in strijd is met de AVG en/of andere toepasselijke wet- of regelgeving.

Wet- en regelgeving:

- Artikel 28 lid 3 (tweede alinea) AVG

2.5 Indien Verwerker in strijd met de Verwerkersovereenkomst en/of de AVG en/of andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens het doel en de middelen van de Verwerking van Persoonsgegevens bepaalt, wordt Verwerker voor die Verwerkingen als Verwerkingsverantwoordelijke beschouwd.

Het doel en de middelen van de verwerking dienen door de instelling te worden bepaald. De rol van de leverancier is om ten behoeve van de instelling persoonsgegevens te verwerken en daarbij binnen de grenzen te blijven die de instelling stelt. Zodra de leverancier zelfstandig doel of middelen van de verwerking gaat bepalen, wordt hij voor die verwerking aangemerkt als verwerkingsverantwoordelijke. Hij dient daarvoor dan ook zelfstandig alle verplichtingen uit de AVG na te komen.

Wet- en regelgeving:

- Artikel 28 lid 10 AVG

ARTIKEL 3. VERLENEN VAN BIJSTAND EN MEDEWERKING

3.1 Verwerker verleent Verwerkingsverantwoordelijke alle benodigde bijstand en medewerking bij het doen nakomen van de op Partijen rustende verplichtingen op grond van de AVG en andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens. Verwerker verleent, voor zover dergelijke bijstand betrekking heeft op de Verwerking van Persoonsgegevens ten behoeve van de uitvoering van de Overeenkomst, Verwerkingsverantwoordelijke in ieder geval dergelijke bijstand met betrekking tot:

(i) De beveiliging van Persoonsgegevens;

(ii) Het uitvoeren van controles en audits;

(iii) Het uitvoeren van DPIA's;

(iv) Voorafgaande raadpleging van de Toezichthoudende autoriteit;

(v) Het voldoen aan verzoeken van de Toezichthoudende autoriteit of een andere overheidsinstantie;

(vi) Het voldoen aan verzoeken van Betrokkenen;

(vii) Het melden van Inbreuken in verband met Persoonsgegevens.

Op grond van de AVG heeft de leverancier de verplichting om de instelling bijstand te verlenen bij de uitvoering van diens wettelijke verplichtingen.

Zo dient de leverancier de instelling bijstand te verlenen bij het beantwoorden van verzoeken van betrokkenen, bij het nakomen van de beveiligingsplicht, het melden van een datalek, het uitvoeren van DPIA's en een voorafgaande raadpleging bij een verwerking met een hoog risico. Deze verplichtingen moeten ingevolge de AVG worden opgenomen in de verwerkersovereenkomst.

Wet- en regelgeving:

- Artikel 28 lid 3 onder e, f en h AVG

3.2 Onder het verlenen van bijstand en medewerking met betrekking tot het voldoen aan verzoeken van Betrokkenen, worden in ieder geval de volgende verplichtingen voor Verwerker verstaan:

3.2.1 Verwerker neemt alle redelijke maatregelen om ervoor te zorgen dat Betrokkene zijn rechten kan uitoefenen.

Op grond van de AVG hebben betrokkenen bepaalde rechten:

- Het recht op informatie (artikel 13 en 14 AVG);
- Het recht tot inzage (artikel 15 AVG);
- Het recht tot rectificatie (artikel 16 AVG);
- Het recht tot gegevenswissing (artikel 17 AVG);
- Het recht tot beperking van de verwerking (artikel 18 AVG);
- Het recht tot dataportabiliteit (artikel 20 AVG);
- Het recht op bezwaar (artikel 21 AVG); en
- Het recht om niet te worden onderworpen aan geautomatiseerde individuele besluitvorming (artikel 22 AVG).

Wanneer een betrokkene een dergelijk verzoek indient bij de instelling zal deze in de praktijk vaak de hulp van de leverancier nodig hebben om hieraan te voldoen. Volgens de AVG dient de verwerkersovereenkomst de verplichting voor de verwerker tot bijstand bij het uitvoeren van deze rechten te bevatten.

De rechten van betrokkenen zijn in het kader van wetenschappelijk onderzoek, statistiek en archivering in het algemeen belang echter beperkt van toepassing. Als de instelling de nodige voorzieningen heeft getroffen om te verzekeren dat de persoonsgegevens uitsluitend voor statistische of wetenschappelijke doeleinden kunnen worden gebruikt of de verwerking van persoonsgegevens deel uitmaakt van archiefbescheiden, kan de instelling de artikelen 15, 16 en 18 van de AVG buiten toepassing laten.

Wet- en regelgeving:

- Artikel 28 lid 3 onder e AVG
- Artikel 44 en 45 Uitvoeringswet en artikel 89 AVG

3.2.2 Indien een Betrokkene met betrekking tot de uitvoering van zijn rechten direct contact opneemt met Verwerker, dan gaat Verwerker hier – behoudens uitdrukkelijke andersluidende instructie van Verwerkingsverantwoordelijke – niet (inhoudelijk) op in, maar bericht Verwerker dit onverwijld aan Verwerkingsverantwoordelijke met een verzoek om nadere instructies.

Ter bescherming van de rechten van betrokkenen en de beveiliging van de persoonsgegevens is het voor de leverancier niet toegestaan om in te gaan op verzoeken van betrokkenen, de instelling is in principe verantwoordelijk voor de afhandeling. Dergelijke verzoeken dienen eerst op rechtmatigheid getoetst te worden door de instelling. In uitzonderingsgevallen kan de instelling een andersluidende instructie geven aan de leverancier.

Wet- en regelgeving:
- Artikel 12 lid 2 AVG

3.2.3 Indien Verwerker de Dienst rechtstreeks aanbiedt aan Betrokkene, is Verwerker verplicht om Betrokkene namens de Verwerkingsverantwoordelijke te informeren over de Verwerking van de Persoonsgegevens van Betrokkene op een wijze die in overeenstemming is met de rechten van Betrokkene.

Artikel 3.2.3 vloeit niet direct voort uit de AVG, maar is toegevoegd aan de Verwerkersovereenkomst om zo aan te sluiten bij de 'GÉANT Data Protection Code of Conduct'. Dit is een door GÉANT ontwikkelde Europese gedragscode, die Service Providers eenzijdig kunnen ondertekenen, om zo aan te geven dat zij voldoen aan de strenge Europese beveiliging- en privacywetgeving. Hierin staat in artikel 2 sub h een dergelijke bepaling zoals geformuleerd in artikel 3.2.3.

De leverancier dient de betrokkene overeenkomstig artikel 12 en 13 van de AVG middels een privacyverklaring te informeren over de verwerking.

3.3 Onder het verlenen van bijstand en medewerking met betrekking tot het voldoen aan verzoeken van de Toezichthoudende autoriteit of een andere overheidsinstantie, worden in ieder geval de volgende verplichtingen voor Verwerker verstaan:

3.3.1 Indien Verwerker een verzoek of een bevel van een Nederlandse en/of buitenlandse overheidsinstantie ontvangt met betrekking tot Persoonsgegevens, waaronder maar niet beperkt tot een verzoek van de Toezichthoudende autoriteit, informeert Verwerker Verwerkingsverantwoordelijke onverwijld, voor zover dat wettelijk is toegestaan. Bij de behandeling van het verzoek of bevel neemt Verwerker alle instructies van Verwerkingsverantwoordelijke in acht en verleent Verwerker alle redelijkerwijs benodigde medewerking aan Verwerkingsverantwoordelijke.

Bij clouddienstverlening worden gegevens niet op locatie van de instelling bewaard. Wanneer autoriteiten een verzoek tot inzage in gegevens doen, dan dient de instelling als verantwoordelijke hierop adequaat te reageren. Wanneer de leverancier een dwingendrechtelijk verzoek of bevel daartoe ontvangt, dan is de leverancier verplicht om de instelling hierover te informeren. Hierbij dienen instructies van de instelling in acht worden genomen, waaronder de behandeling van het verzoek of bevel over te laten aan de instelling. Als verantwoordelijke van de (persoons)gegevens dient de instelling het aanspreekpunt voor dergelijk verzoeken of bevelen te zijn.

3.3.2 Indien het Verwerker wettelijk is verboden om te voldoen aan zijn verplichtingen op grond van artikel 3.3.1, behartigt Verwerker de redelijke belangen van Verwerkingsverantwoordelijke. Hieronder wordt in ieder geval verstaan:

3.3.2.1 Verwerker laat juridisch toetsen in hoeverre: (i) Verwerker wettelijk verplicht is om aan het verzoek of bevel te voldoen; en (ii) het Verwerker daadwerkelijk is verboden om aan zijn verplichtingen jegens Verwerkingsverantwoordelijke op grond van artikel 3.3.1 te voldoen.

3.3.2.2 Verwerker werkt alleen mee aan het verzoek of bevel indien Verwerker hiertoe wettelijk verplicht is en waar mogelijk maakt Verwerker (in rechte) bezwaar tegen het verzoek of bevel of het verbod om Verwerkingsverantwoordelijke hierover te informeren of de instructies van Verwerkingsverantwoordelijke op te volgen.

3.3.2.3 Verwerker verstrekt niet meer Persoonsgegevens dan strikt noodzakelijk om aan het verzoek of bevel te voldoen.

3.3.2.4 Verwerker onderzoekt indien sprake is van doorgifte in de zin van artikel 8 de mogelijkheden om te voldoen aan de artikelen 44 tot en met 46 AVG.

In sommige gevallen is het voor de leverancier door dwingendrechtelijke wet- en regelgeving verboden om te voldoen aan artikel 3.3.1. In die gevallen dient de beveiliging van de gegevens alsnog gewaarborgd te worden. Daarom is de leverancier verplicht een aantal handelingen uit te voeren die normaliter door de instelling worden uitgevoerd.

Met het uitvoeren van de genoemde punten wordt de bescherming van de persoonsgegevens zoveel als mogelijk gewaarborgd.

Artikelen 44 t/m 46 AVG gaan over doorgifte van gegevens naar derde landen. Dit is alleen toegestaan als er sprake is van een van de in de artikelen genoemde uitzonderingen. Zie artikel 8 van dit Instructiemodel voor een verdere toelichting van deze artikelen.

ARTIKEL 4. TOEGANG TOT PERSOONSGEGEVENS

4.1 Verwerker beperkt de toegang tot Persoonsgegevens aan Medewerkers, Sub-verwerkers, Derden en andere Ontvangers van Persoonsgegevens tot een noodzakelijk minimum.

4.2 Verwerker verschaft uitsluitend toegang aan die Medewerkers voor wie ter uitvoering van de Overeenkomst deze toegang tot Persoonsgegevens noodzakelijk is. De categorieën Medewerkers zijn in Bijlage A gespecificeerd.

Ter beveiliging van de persoonsgegevens in het kader van de principes van integriteit en vertrouwelijkheid, dient in de verwerkersovereenkomst te worden vastgelegd welke medewerkers (functionarissen) of welke groepen medewerkers welke verwerking mogen uitvoeren ten aanzien van de persoonsgegevens. Er geldt een expliciet verbod op het uitvoeren van verwerkingen door andere medewerkers dan de genoemde (groepen) medewerkers in dit artikel. De verwerkersovereenkomst dient te borgen dat deze medewerkers aan geheimhouding zijn gebonden. Werknemers zijn van rechtswege al gebonden aan geheimhouding ingevolge artikel 272 Wetboek van Strafrecht.

Wet- en regelgeving:

- Artikel 28 lid 3 onder b en artikel 32 lid 4 AVG
- Artikel 29 AVG

4.3 Verwerker verschaft Sub-verwerkers geen toegang tot Persoonsgegevens zonder voorafgaande algemene of specifieke Schriftelijke toestemming van Verwerkingsverantwoordelijke. Algemene Schriftelijke toestemming voor het inschakelen van Sub-verwerkers is slechts verleend indien dit expliciet in Bijlage A is opgenomen. Specifieke toestemming voor het inschakelen van Sub-verwerkers is slechts verleend aan Sub-verwerkers die in Bijlage A zijn gespecificeerd.

Op grond van de AVG mag de leverancier (verwerker) geen andere sub-verwerkers inschakelen, zonder voorafgaande specifieke of algemene schriftelijke toestemming van de instelling (de verwerkingsverantwoordelijke):

1. *Specifieke toestemming* is gericht op een specifieke sub-verwerker. Indien er een sub-verwerker wijzigt, zal (opnieuw) specifieke toestemming nodig zijn van de instelling voor het inschakelen van een nieuwe sub-verwerker.
2. Bij *algemene toestemming* hoeft de instelling niet voor elke nieuwe sub-verwerker vooraf schriftelijke toestemming te geven. Wel dient de instelling vooraf te worden geïnformeerd over de in te schakelen sub-verwerkers en heeft hij het recht om bezwaar te maken.

In bijlage A kan worden vastgelegd voor welke soort toestemming wordt gekozen.

Wet- en regelgeving:

- Artikel 28 lid 2 AVG

4.4 De Sub-verwerkers die Verwerker inschakelt ter uitvoering van de Overeenkomst, zijn opgenomen in Bijlage A.

Op grond van de AVG is het belangrijk dat de instelling te allen tijde een overzicht heeft van de door de leverancier ingeschakelde sub-verwerkers. Het overzicht in bijlage A moet, in geval van een wijziging, zowel bij specifieke als bij algemene toestemming tijdig worden aangepast. Hierdoor zal bijlage A altijd een compleet overzicht bieden van de door de leverancier ingeschakelde sub-verwerkers.

4.5 Verwerker licht Verwerkingsverantwoordelijke in geval van algemene Schriftelijke toestemming voor het inschakelen van Sub-verwerkers uiterlijk drie (3) maanden voorafgaand aan beoogde veranderingen inzake de toevoeging, vervanging of wijziging van Sub-verwerker(s) en de ten gevolge hiervan noodzakelijke wijziging van Bijlage A, Schriftelijk in, waarbij de Verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen Schriftelijk bezwaar te maken, binnen één (1) maand nadat Verwerkingsverantwoordelijke door Verwerker over de beoogde verandering is ingelicht. Partijen treden hierop in onderhandeling.

Indien de instelling het niet eens is met de inschakeling van een bepaalde sub-verwerker heeft zij het recht om hier bezwaar tegen te maken. Bij bezwaar zal de leverancier in principe de verandering niet mogen doorvoeren. Partijen zullen dan in overleg treden om tot een oplossing te komen. Als partijen niet tot een oplossing kunnen komen, is één van de mogelijkheden dat de verwerkersovereenkomst met wederzijds goedvinden wordt beëindigd.

De mogelijkheid van bezwaar is nodig, omdat de instelling, als verwerkingsverantwoordelijke, te allen tijde toezicht moet kunnen houden op de verwerking.

Wet- en regelgeving:

- Artikel 28 lid 2 AVG

4.6 De algemene of specifieke toestemming van Verwerkingsverantwoordelijke voor het inschakelen van Sub-verwerkers laat de verplichtingen voor Verwerker voortvloeiende uit de Verwerkersovereenkomst, waaronder maar niet beperkt tot artikel 8, onverlet. Verwerkingsverantwoordelijke kan zijn algemene of specifieke Schriftelijke toestemming voor het inschakelen van Sub-verwerkers intrekken, indien Verwerker niet of niet langer voldoet aan de verplichtingen uit de Verwerkersovereenkomst, de AVG en/of andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

4.7 Verwerker legt de in de Verwerkersovereenkomst opgenomen verplichtingen op aan de door Verwerker ingeschakelde Sub-verwerkers door middel van een Schriftelijke overeenkomst.

Op grond van de AVG is de leverancier verplicht bij overeenkomst of andere rechtshandeling afspraken te maken met sub-verwerkers over de verplichtingen omtrent de verwerking van persoonsgegevens. Deze verplichtingen dienen hetzelfde te zijn als de afspraken tussen de instelling en de leverancier.

Wet- en regelgeving:

- Artikel 28 lid 4 AVG

Verwerker garandeert dat de tot het verwerken van de Persoonsgegevens gemachtigde personen en andere Ontvangers van Persoonsgegevens zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden.

De verwerkersovereenkomst dient te waarborgen dat de tot het verwerken van de persoonsgegevens gemachtigde personen aan geheimhouding zijn gebonden.

Wet- en regelgeving:
- Artikel 28 lid 3 sub b AVG

4.8 Verwerker verstrekt op verzoek van Verwerkingsverantwoordelijke bewijs dat Verwerker, door Verwerker ingeschakelde Sub-verwerkers, de tot het verwerken van de Persoonsgegevens gemachtigden personen en andere Ontvangers van Persoonsgegevens, voldoen aan artikel 4.7.

Omdat de instelling als verwerkingsverantwoordelijke moet kunnen controleren of de verwerking geschied in overeenstemming met de AVG, is de leverancier verplicht om op verzoek van de instelling onverwijld bewijs te verstrekken van de overeenkomst met de sub-verwerkers en van de afspraken omtrent vertrouwelijkheid met de tot het verwerken van de persoonsgegevens gemachtigde personen en andere ontvangers van persoonsgegevens.

Wet- en regelgeving:
- Artikel 28 lid 3 onder h en lid 4 AVG

4.9 Verwerker blijft ten aanzien van de Verwerkingsverantwoordelijke volledig verantwoordelijk en volledig aansprakelijk voor het nakomen van de verplichtingen door de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers en/of Ontvangers, voortvloeiende uit de AVG en/of andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens en de verplichtingen voortvloeiende uit de Overeenkomst en de Verwerkersovereenkomst.

De leverancier zal tegenover de instelling volledig verantwoordelijk blijven voor de nakoming van de verplichtingen van ingeschakelde sub-verwerkers.

Wet- en regelgeving:
- Artikel 28 lid 4 AVG

ARTIKEL 5. BEVEILIGING

5.1 Verwerker treft passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, opdat de Verwerking aan de vereisten van de AVG en andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet en de bescherming van de rechten van Betrokkenen is gewaarborgd. Verwerker treft hiertoe tenminste de technische en organisatorische maatregelen die zijn opgenomen in Bijlage B.

Onder de AVG heeft de leverancier als verwerker een zelfstandige verplichting om zorg te dragen voor een adequate beveiliging van persoonsgegevens. Daarnaast dient de instelling als verwerkingsverantwoordelijk erop toe te zien dat leveranciers afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden, opdat de verwerking aan de wettelijke vereisten voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd.

Ten aanzien van de beveiliging geldt dat de instelling op basis van een risicoanalyse moet bepalen of de leverancier voldoende waarborgen biedt voor de bescherming van persoonsgegevens. De gevraagde garanties dienen met name betrekking te hebben op het gebied van deskundigheid, betrouwbaarheid en middelen.

Meer informatie over passende beveiliging: zie Handreiking Beveiligingsmaatregelen, Bijlage C Juridisch Normenkader:
https://www.surf.nl/binaries/content/assets/surf/nl/2018/jnk-2018/surf_c-handreiking-beveiligingsmaatregelen---bijlage-c---versie-mei-2018.pdf.

Wet- en regelgeving:
- Artikel 28 lid 1, lid 3 onder c en artikel 32 AVG
- Overweging 81 bij de AVG

5.2 Bij de beoordeling van het passende beveiligingsniveau houdt Verwerker rekening 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, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

De beveiligingsmaatregelen dienen een ‘passend niveau’ van beveiliging te waarborgen, waarbij rekening moet worden gehouden 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.

Daarnaast dient bij de beoordeling van wat als ‘passend’ moet worden beschouwd, de nadruk te liggen bij de verwerkingsrisico’s: wat kan er misgaan? Het gaat hierbij zowel om onvoorziene verwerkingen (‘per ongeluk’) als om verwerkingen die opzettelijk in strijd zijn met de AVG.

Wet- en regelgeving:
- Artikel 32 lid 1 en lid 2 AVG

5.3 Verwerker legt zijn beveiligingsbeleid Schriftelijk vast. Op verzoek van Verwerkingsverantwoordelijke verschaft Verwerker bewijs van een Schriftelijk beveiligingsbeleid bij Verwerker.

Omdat de instelling als verwerkingsverantwoordelijke moet kunnen controleren of de persoonsgegevens adequaat worden beveiligd is de leverancier verplicht om op verzoek van de instelling onverwijld bewijs van een schriftelijk beveiligingsbeleid te verstrekken.

Wet- en regelgeving:
- Artikel 28 lid 3 onder h AVG

ARTIKEL 6. AUDIT

6.1 Verwerker is verplicht conform artikel 6.2 periodiek een onafhankelijke, externe deskundige een audit te laten uitvoeren ten aanzien van de organisatie van Verwerker, teneinde aan te tonen dat Verwerker aan het bepaalde in de Verwerkersovereenkomst, de AVG en andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet.

Onder de AVG heeft de verwerker een zelfstandige verantwoordelijkheid om passende technische en organisatorische maatregelen te treffen. Een periodieke audit is een passende wijze voor een verwerker om aan te tonen dat hij voldoet aan zijn wettelijke verplichtingen uit de AVG.

Wet- en regelgeving:
- Artikel 28 lid 3 onder c en f en artikel 32 lid 1 AVG

6.2 Verwerkingsverantwoordelijke legt de frequentie van de door Verwerker uit te voeren periodieke audit, zoals bedoeld in artikel 6.1, vast in Bijlage A.

6.2.1 Verwerker verricht tenminste eenmaal per twee jaar een periodieke audit, zoals bedoeld in artikel 6.1, tenzij artikel 6.2.2 of 6.2.3 van toepassing is.

6.2.2 Indien Bijzondere categorieën Persoonsgegevens worden verwerkt of een Verwerking wordt verricht die een hoog risico inhoudt voor de rechten en vrijheden van de Betrokkenen, verricht Verwerker tenminste eenmaal per jaar een periodieke audit, zoals bedoeld in artikel 6.1.

6.2.3 Indien Verwerker uitsluitend verwerkingen verricht die een laag risico inhouden voor de rechten en vrijheden van Betrokkenen, is Verwerker niet gehouden tot het verrichten van een periodieke audit, zoals bedoeld in artikel 6.1.

Zoals uit artikel 6.2 blijkt is de frequentie van de periodieke audits afhankelijk van het soort persoonsgegevens dat wordt verwerkt. Het combineren van gegevens kan van invloed zijn op de risicoklasse van de gegevens. In sommige gevallen zal het combineren van gegevens kunnen leiden tot een hogere risicoklasse.

Er zijn drie soorten risicoklassen:

- Laag: onder deze categorie vallen alleen persoonsgegevens waarvan algemeen aanvaard is dat deze, bij het beoogde gebruik, geen risico opleveren voor de betrokkene. Het kan hier gaan om gegevens die publiekelijk toegankelijk zijn, maar dit hoeft niet altijd het geval te zijn. Denk bijvoorbeeld aan een naam, zakelijk e-mailadres of een beroep.
  - *Geen periodieke audit verplichting.*
- Midden: hier gaat het om persoonsgegevens die niet vallen onder de risicoklasse 'laag' of onder de categorie 'Bijzondere Persoonsgegevens'. Denk hierbij bijvoorbeeld aan de inschrijving van een student of locatiegegevens.
  - *De audit verplichting is één keer per twee jaar.*
- Hoog: hier gaat het in ieder geval om persoonsgegevens die vallen in de categorie 'Bijzonder Persoonsgegevens' (artikel 9 AVG), waar onder andere politieke opvattingen, gegevens waaruit ras of etnische afkomst blijken, genetische en biometrische gegevens en strafrechtelijke gegevens onder vallen. Ook het BSN en onderwijsnummer vallen onder de risicoclassificatie Hoog.
  - *De auditverplichting is jaarlijks.*

Ook voorafgaand aan het sluiten van de overeenkomst dient een dergelijk onderzoek te hebben plaatsgevonden zodat de instelling de dienstverlening door de leverancier heeft onderzocht.

Meer informatie over de auditverplichting, zie Handreiking Auditverplichting, Bijlage D Juridisch Normenkader:
https://www.surf.nl/binaries/content/assets/surf/nl/2018/jnk-2018/surf_d-handreiking-auditverplichting---bijlage-d---versie-mei-2018.pdf.

Zie ook 'Recommendations for a methodology of the assessment of severity of personal data breaches' afkomstig van Enisa voor een nadere toelichting van de risicoklassen.

6.3 Verwerker is verplicht de bevindingen van de onafhankelijke, externe deskundige uit de periodieke audit, op verzoek aan Verwerkingsverantwoordelijke ter beschikking te stellen in de vorm van een verklaring, waarin de deskundige:

(i) Een oordeel geeft over de kwaliteit van de door Verwerker getroffen technische en organisatorische beveiligingsmaatregelen met betrekking tot de Verwerkingen die Verwerker ten behoeve van Verwerkingsverantwoordelijke verricht;

(ii) Verwerkingsverantwoordelijke informeert over de overige bevindingen die relevant zijn voor nakoming van de Verwerkersovereenkomst, de AVG en andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

Als verwerkingsverantwoordelijke is de instelling verplicht om toe te zien op een adequate beveiliging door de leverancier. Een van de instrumenten die door de Autoriteit Persoonsgegevens hiervoor wordt voorgeschreven is een verklaring van een onafhankelijk, externe deskundige: een Third Party Memorandum (TPM). Een TPM is een verklaring waarin de onafhankelijke externe deskundige een oordeel geeft over de maatregelen die de leverancier heeft getroffen. De TPM wordt opgesteld in opdracht van de leverancier en wordt verstrekt aan de instelling die gebruik maakt van de diensten van de leverancier. Het doel van het verstrekken van een TPM is om de instelling inzicht te bieden in de getroffen maatregelen van de leverancier, zonder dat iedere instelling daar zelf onderzoek hoeft te (laten) doen.

6.4 Verwerkingsverantwoordelijke heeft het recht op zijn verzoek een audit te laten uitvoeren door een door Verwerkingsverantwoordelijke gemachtigde deskundige, ten aanzien van de organisatie van Verwerker, teneinde aan te tonen dat Verwerker aan het bepaalde in de Verwerkersovereenkomst, de AVG en andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet. Verwerkingsverantwoordelijke kan maximaal éénmaal per jaar gebruik maken van het recht op zijn verzoek een audit te laten uitvoeren bij Verwerker, zoals bedoeld in dit artikellid, of vaker bij een concreet vermoeden dat Verwerker de Verwerkersovereenkomst en/of de AVG en/of andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, niet nakomt. Verwerkingsverantwoordelijke stelt Verwerker ten minste 14 (veertien) dagen voor aanvang van de audit Schriftelijk in kennis. De audit mag de normale bedrijfsactiviteiten van Verwerker niet onredelijk verstoren.

De leverancier is ingevolge de AVG verplicht mee te werken aan audits door de instelling of een door de instelling gemachtigde controleur, ter verificatie dat hij voldoet aan de verwerkersovereenkomst en meer algemeen de AVG.

Wet- en regelgeving:
- Artikel 28 lid 3 onder h AVG

6.5 De kosten van de periodieke audit komen voor rekening van Verwerker. De kosten van de audit op verzoek van Verwerkingsverantwoordelijke komen voor rekening van Verwerkingsverantwoordelijke, tenzij uit de bevindingen van de audit blijkt dat Verwerker de bepalingen uit de Verwerkersovereenkomst en/of de AVG en/of andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens niet is nagekomen.

Wanneer de instelling een redelijk vermoeden heeft van schending van gemaakte afspraken door de leverancier, dient de instelling dit vermoeden te onderzoeken. Hierbij gaat het om een (beperkte) kwaliteitstoetsing. De uitvoering van dit onderzoek wordt in eerste instantie bekostigd door de instelling zelf. Wanneer uit het onderzoek blijkt dat er inderdaad sprake is van een schending van gemaakte afspraken door leverancier, dan kan de instelling de kosten voor het onderzoek verhalen op de leverancier.

De kosten van de periodieke audit uit artikel 6 lid 1 van de verwerkersovereenkomst komen voor rekening van de leverancier.

6.6 Indien tijdens een audit wordt vastgesteld dat Verwerker niet aan het bepaalde in de Verwerkersovereenkomst en/of de AVG en/of andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet, neemt Verwerker onverwijld

alle redelijkerwijs noodzakelijke maatregelen om te zorgen dat Verwerker hieraan alsnog voldoet. De bijbehorende kosten komen voor rekening van Verwerker.

ARTIKEL 7. INBREUK IN VERBAND MET PERSOONSGEGEVENS

7.1 Verwerker informeert Verwerkingsverantwoordelijke zonder onredelijke vertraging en uiterlijk binnen 24 uur na kennisneming, over een Inbreuk in verband met Persoonsgegevens. Verwerker informeert Verwerkingsverantwoordelijke via de contactpersoon en de contactgegevens van Verwerkingsverantwoordelijke zoals opgenomen in Bijlage A en ten minste ten aanzien van alle informatie zoals die blijkt uit het meest recente formulier datalekken van de Autoriteit Persoonsgegevens, welke te vinden is op de website van de Autoriteit Persoonsgegevens. Verwerker garandeert dat de verstrekte informatie, voor zover bekend bij Verwerker op dat moment, volledig, correct en accuraat is.

Volgens de AVG moet de instelling datalekken die vallen onder de meldplicht binnen 72 uur nadat hij er kennis van heeft genomen melden bij de Autoriteit Persoonsgegevens. Daarbij horen ook datalekken die plaatsvinden bij leveranciers of hulpleveranciers van de leveranciers. Aangezien het de verantwoordelijkheid van de instelling is om te bepalen of een bepaald datalek gemeld dient te worden of niet, is het belangrijk dat de leverancier alle inbreuken meldt.

De instelling moet dus tijdig op de hoogte worden gebracht van een potentieel datalek, om te kunnen beoordelen of er gemeld moet worden. Daarom is in dit artikel geregeld dat de leverancier binnen 24 uur na ontdekking van het datalek dit meldt aan de instelling. Hieronder vallen ook datalekken van eventuele ingeschakelde sub-verwerkers. Daarom is er ook de plicht voor de leverancier om ook met sub-verwerkers afspraken te maken over de meldplicht datalekken. Omdat de keten van betrokken partijen hier langer is, geldt voor die sub-verwerkers dat zij onverwijld het datalek dienen te melden aan de leverancier, om het mogelijk te houden dat de instelling binnen 72 uur kan melden aan de Autoriteit Persoonsgegevens.

De leverancier moet melding maken bij de instelling van alle informatie zoals die blijkt uit het meest recente formulier datalekken van de Autoriteit Persoonsgegevens.

Wet- en regelgeving:
- Artikel 28 lid 3 onder f en artikel 33 AVG
- Guidelines meldplicht datalekken

7.2 Indien en voor zover het voor Verwerker niet mogelijk is om alle informatie uit het formulier datalekken van de Autoriteit Persoonsgegevens gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging en in overeenstemming met artikel 7.1, in stappen worden verstrekt aan Verwerkingsverantwoordelijke.

Wet- en regelgeving:
- Artikel 33 lid 4 AVG

7.3 Verwerker heeft adequaat beleid en adequate procedures ingericht om:

(i) Inbreuken in verband met Persoonsgegevens in een zo vroeg mogelijk stadium te detecteren;

(ii) Verwerkingsverantwoordelijke over een Inbreuk in verband met Persoonsgegevens in overeenstemming met artikel 7.1 te informeren;

(iii) Adequaat en onmiddellijk op een Inbreuk in verband met Persoonsgegevens te reageren;

(iv) (verdere) onbevoegde kennisneming, wijziging, en verstrekking dan wel anderszins onrechtmatige Verwerking te voorkomen of te beperken en herhaling hiervan te voorkomen.

Op verzoek van Verwerkingsverantwoordelijke verschaft Verwerker informatie over en inzage in dit door Verwerker ingerichte beleid en deze door Verwerker ingerichte procedures.

7.4 Verwerker houdt Schriftelijk een register bij van alle Inbreuken in verband met Persoonsgegevens die betrekking hebben op of verband houden met de (uitvoering van de) Overeenkomst, met inbegrip van de feiten omtrent de Inbreuk in verband met Persoonsgegevens, de gevolgen daarvan en de getroffen corrigerende maatregelen. Op verzoek van Verwerkingsverantwoordelijke verschaft Verwerker Verwerkingsverantwoordelijke een afschrift van dit register.

Op grond van de AVG heeft de instelling een verplichting om een register bij te houden van ieder datalek, ongeacht of het lek moet worden gemeld of niet. De leverancier heeft een wettelijke verplichting om de instelling hierbij bijstand te verlenen.

Wet- en regelgeving:
- Artikel 33 lid 5 en artikel 28 lid 3 onder f AVG

7.5 Verwerker onthoudt zich van het doen van meldingen omtrent Inbreuken in verband met Persoonsgegevens aan de Toezichthoudende autoriteit en/of de getroffen Betrokkenen, tenzij op uitdrukkelijk Schriftelijk verzoek van Verwerkingsverantwoordelijke.

Op grond van de AVG is de instelling, als verwerkingsverantwoordelijke, degene die in geval van een datalek de afweging moet maken of er sprake is van een (hoog) risico voor de rechten en vrijheden van natuurlijke personen en de melding moet maken aan de Autoriteit Persoonsgegevens en eventueel de betrokkenen. Het is niet de bedoeling dat de leverancier dit doet.

Wet- en regelgeving:
- Artikel 33 en artikel 34 AVG

ARTIKEL 8. DOORGIFTE VAN PERSOONSGEGEVENS

8.1 Persoonsgegevens mogen enkel worden doorgegeven aan landen buiten de Europese Economische Ruimte of internationale organisaties indien sprake is van een passend beschermingsniveau, in overeenstemming wordt gehandeld met de artikelen 44 tot en met 49 AVG en Verwerkingsverantwoordelijke hiervoor specifieke Schriftelijke toestemming heeft verleend. Deze specifieke Schriftelijke toestemming is slechts verleend indien dit is opgenomen in Bijlage A.

Ingevolge de AVG moeten er in de verwerkersovereenkomst afspraken zijn gemaakt omtrent doorgifte van persoonsgegevens naar derde landen. In de Model Verwerkersovereenkomst is ervoor gekozen dat de leverancier voorafgaande schriftelijke toestemming nodig heeft van de instelling, voordat de leverancier een derde partij buiten de EER (Europese Economische Ruimte: alle landen van de EU plus Noorwegen, Liechenstein en IJsland) mag inschakelen. Als partijen in afwijking hiervan er toch voor kiezen om deze voorafgaande toestemming te vervangen door de mogelijkheid voor de instelling om bezwaar te maken, is het belangrijk dat daar voldoende afspraken over worden vastgelegd. Denk daarbij onder meer aan het tijdig schriftelijk inlichten van de instelling over de beoogde verandering inzake de doorgifte buiten de EER en de mogelijkheid voor de instelling om daartegen bezwaar te maken.

Het is onder de AVG slechts in drie situaties toegestaan om persoonsgegevens te verwerken in derde landen. Als derde land wordt aangemerkt elk land buiten de EER. De drie mogelijkheden voor doorgifte van persoonsgegevens buiten de EER betreffen:

1. Indien het land door de Europese Commissie is aangemerkt als een land met een adequaat beschermingsniveau (artikel 45 AVG). Deze lijst is te vinden via: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

   Verwerking van persoonsgegevens in de VS: de VS wordt slechts aangemerkt als een adequaat land, mits men uitsluitend persoonsgegevens doorgeeft aan bedrijven die een zogenaamd Privacy Shield hebben (wegens een op het moment van schrijven van dit document lopende procedure bij het Hof van Justitie van de Europese Unie tegen het Privacy Shield, is het echter niet zeker of deze overeenkomst in stand zal blijven).

2. Indien sprake is van een van de ‘passende waarborgen’ of Binding Corporate Rules (artikel 46 en 47 AVG). Dit betreffen de volgende maatregelen:
   a. Binding Corporate Rules;
   b. modelcontract van de Europese Commissie;
   c. modelcontract van de Autoriteit Persoonsgegevens;
   d. een zelf opgestelde en door de Autoriteit Persoonsgegevens goedgekeurde overeenkomst;
   e. gedragscode;
   f. certificering.

3. Indien sprake is van één van de specifieke situaties uit artikel 49 lid 1 AVG. Dit betreffen:
   a. uitdrukkelijke toestemming van de betrokkene;
   b. als de doorgifte noodzakelijk is voor het aangaan of uitvoeren van een overeenkomst (restrictief uitgelegd);
   c. als doorgifte noodzakelijk is voor gewichtige redenen van algemeen belang;
   d. als doorgifte is voor het instellen, uitoefenen of onderbouwen van een rechtsvordering;
   e. als doorgifte noodzakelijk is voor een vitaal belang van een persoon;
   f. voor een bij wet ingesteld register;
   g. de zogenaamde ‘incidentele doorgifte’ van artikel 49 lid 1 onder g AVG.

Wet- en regelgeving:

- Artikel 28 lid 3 onder a en artikel 44 t/m 50 AVG

8.2 Verwerker dient op verzoek van Verwerkingsverantwoordelijke aan te tonen dat aan de vereisten zoals opgenomen in artikel 8.1 is voldaan.

8.3 De doorgiften van Persoonsgegevens buiten de Europese Economische Ruimte of aan internationale organisaties ter uitvoering van de Overeenkomst, zijn nader omschreven in Bijlage A. Verwerker is uitsluitend gerechtigd tot deze in Bijlage A gespecificeerde doorgiften aan derde landen of internationale organisaties, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot Verwerking verplicht. In dat geval stelt Verwerker Verwerkingsverantwoordelijke voorafgaand aan de Verwerking Schriftelijk op de hoogte van deze bepaling, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

ARTIKEL 9. VERTROUWELIJKHEID VAN PERSOONSGEGEVENS

9.1 Alle Persoonsgegevens worden als vertrouwelijke gegevens gekwalificeerd en dienen als zodanig te worden behandeld.

9.2 Partijen houden alle Persoonsgegevens geheim en maken deze op geen enkele wijze verder intern of extern bekend, behalve voor zover:

(i) Bekendmaking en/of verstrekking van de Persoonsgegevens in het kader van de uitvoering van de Overeenkomst of Verwerkersovereenkomst noodzakelijk is;

(ii) Enig voorschrift van dwingend Unie- of lidstatelijk recht of een daarop gebaseerde rechterlijke uitspraak van een bevoegde rechtbank, Partijen tot bekendmaking, verstrekking en/of doorgifte van die Persoonsgegevens verplicht, waarbij Partijen hetgeen is bepaald in artikel 3 in acht nemen;

(iii) Bekendmaking en/of verstrekking van die Persoonsgegevens geschiedt met voorafgaande Schriftelijke toestemming van de andere Partij.

Hoewel vertrouwelijkheid verder reikt dan alleen persoonsgegevens (bedrijfsgevoelige gegevens kunnen bijvoorbeeld ook vertrouwelijk zijn), is in deze Model Verwerkersovereenkomst ook een vertrouwelijkheidsbepaling opgenomen. Daarnaast heeft de Autoriteit Persoonsgegevens in een nieuwsbericht uit 2016 aangegeven dat een geheimhoudingsplicht onderdeel moet zijn van een verwerkersovereenkomst.

Zie:
- https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-eist-betere-afspraken-over-digitaliseren-pati%C3%ABntdossiers.
- Richtlijn betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie tegen het onrechtmatige verkrijgen, gebruiken en openbaar maken daarvan (Pb EU 2016, L157) en de Nederlandse Wet bescherming bedrijfsgeheimen.

ARTIKEL 10. AANSPRAKELIJKHEID

10.1 Een Partij kan geen beroep doen op een aansprakelijkheidsbeperking, die is opgenomen in de Overeenkomst of andere tussen Partijen bestaande overeenkomst of regeling, ten aanzien van een door de andere Partij ingestelde:

a. verhaalsactie op grond van artikel 82 AVG; of

b. schadevergoedingsactie uit hoofde van de Verwerkersovereenkomst, indien en voor zover de actie bestaat uit verhaal van een aan de Toezichthoudende

autoriteit betaalde geldboete die geheel of gedeeltelijk toerekenbaar is aan de andere Partij.

Het bepaalde in dit artikel laat onverlet de rechtsmiddelen die de aangesproken Partij op grond van de geldende wet- of regelgeving ter beschikking staat.

10.2 Iedere Partij is verplicht de andere Partij zonder onnodige vertraging op de hoogte te stellen van een (mogelijke) aansprakelijkstelling of het (mogelijk) opleggen van een boete door de Toezichthoudende autoriteit, beiden in verband met de Verwerkersovereenkomst. Iedere Partij is in redelijkheid verplicht de andere Partij informatie te verstrekken en/of ondersteuning te verlenen ten behoeve van het voeren van verweer tegen een (mogelijke) aansprakelijkstelling of boete, zoals bedoeld in de vorige volzin. De Partij die informatie verstrekt en/of ondersteuning verleent, is gerechtigd om eventuele redelijke kosten dienaangaande in rekening te brengen bij de andere Partij, Partijen informeren elkaar zo veel mogelijk vooraf over deze kosten.

Op grond van het Burgerlijk Wetboek is een partij die tekortschiet in de nakoming van een overeenkomst, aansprakelijk voor de schade die daaruit voortvloeit. In deze Model Verwerkersovereenkomst is ervoor gekozen om aan te sluiten bij de aansprakelijkheidsbepaling uit de hoofdovereenkomst tussen partijen. In een tweetal gevallen is het echter niet mogelijk voor een partij om zich op een eventuele beperking van aansprakelijkheid uit de hoofdovereenkomst te beroepen:

1. Als de andere partij een verhaalsactie op grond van artikel 82 AVG instelt.
2. Als de andere partij een schadevergoedingsactie uit hoofde van de verwerkersovereenkomst instelt, als de actie bestaat uit verhaal van een aan de toezichthoudende autoriteit betaalde geldboete die geheel of gedeeltelijk toerekenbaar is aan de andere partij.

Artikel 82 lid 1, 2 en 4 AVG stelt dat de betrokkene het recht heeft om voor eventuele schadevergoeding zowel aan te kloppen bij de instelling als bij de leverancier, onafhankelijk van de vraag bij wie de schuld lag. Lid 5 van dit artikel introduceert vervolgens de mogelijkheid om een onderling verhaalsrecht overeen te komen tussen leverancier en instelling.

Daarnaast is het belangrijk dat de leverancier afdoende verzekerd is. Verzekeringen kunnen onderling sterk verschillen en niet alle verzekeringen zijn geschikt voor cloudleveranciers. Bij het beoordelen van de verzekering van de leverancier, is het belangrijk om in ieder geval op de volgende punten te letten:

- De hoogte van de dekking.
- Wat er wordt gedekt door de verzekering en wat er wordt uitgesloten van dekking (bijvoorbeeld ‘verlies van gegevens’ en ‘kosten voor meldplicht’).

Wet- en regelgeving:

- Artikel 28 lid 4 AVG
- Artikel 82 lid 1, lid 2 en lid 4 AVG

ARTIKEL 11. WIJZIGING

11.1 Verwerker is verplicht Verwerkingsverantwoordelijke onmiddellijk te informeren over voorgenomen wijzigingen in de Dienst, de uitvoering van de Overeenkomst en de uitvoering van de Verwerkersovereenkomst die betrekking hebben op de Verwerking van Persoonsgegevens en die (mogelijk) een wijziging van de Verwerkersovereenkomst en/of de Bijlagen vereisen. Hieronder wordt in ieder geval verstaan:

(i) Wijzigingen die invloed (kunnen) hebben op de te verwerken (categorieën) Persoonsgegevens;

(ii) Wijziging van de middelen waarmee de Persoonsgegevens worden verwerkt;

(iii) Het inschakelen van andere Sub-verwerkers;

(iv) Wijziging in de doorgifte van Persoonsgegevens.

11.2 Verwerker is pas gerechtigd tot het uitvoeren van een wijziging in de Dienst, een wijziging in de uitvoering van de Overeenkomst, een wijziging in de uitvoering van de Verwerkersovereenkomst en/of een wijziging die aanpassing van Bijlage A of Bijlage B tot gevolg heeft, indien Verwerkingsverantwoordelijke daaraan voorafgaand Schriftelijk toestemming voor deze wijziging(en) heeft gegeven. Onder een wijziging in de Dienst wordt verstaan een substantiële wijziging die gevolgen kan hebben voor de Verwerking van Persoonsgegevens. Verwerker kan in afwijking van voorgaande zonder voorafgaande Schriftelijke toestemming van Verwerkingsverantwoordelijke direct noodzakelijke verbeteringen uitvoeren, bijvoorbeeld met betrekking tot adequate beveiliging van de dienst. Verwerker zal Verwerkingsverantwoordelijke zo spoedig mogelijk informeren over de wijziging.

Om de taak als verwerkingsverantwoordelijke uit te kunnen voeren dient de instelling zich ervan te vergewissen dat persoonsgegevens overeenkomstig het vooraf bepaalde risiconiveau worden verwerkt. Wanneer de verwerking (de dienstverlening van de leverancier) wijzigt, moet de instelling voorafgaand aan de wijziging kunnen controleren of de verwerking overeenkomstig het passende niveau plaatsvindt.

Wet- en regelgeving:
- Artikel 28 lid 1 AVG

11.3 Wijzigingen die betrekking hebben op de Verwerking van Persoonsgegevens mogen nooit tot gevolg hebben dat Verwerkingsverantwoordelijke niet kan voldoen aan de AVG en/of andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

11.4 In geval van nietigheid of vernietigbaarheid van één of meer bepalingen van de Verwerkersovereenkomst, blijven de overige bepalingen onverkort van kracht.

ARTIKEL 12. DUUR EN BEËINDIGING

12.1 De duur van de Verwerkersovereenkomst is gelijk aan de duur van de Overeenkomst. De Verwerkersovereenkomst is niet los van de Overeenkomst te beëindigen. Bij beëindiging van de Overeenkomst eindigt de Verwerkersovereenkomst van rechtswege en vice versa.

Let op: middels deze bepaling wordt de duur van de overeenkomst en duur van de verwerkersovereenkomst aan elkaar gekoppeld. Bij beëindigd van de overeenkomst eindigt automatisch ook de verwerkersovereenkomst en vice versa.

In sommige gevallen zal dit niet wenselijk zijn, bijvoorbeeld als de overeenkomst een breder toepassingsbereik heeft dan de verwerkersovereenkomst. In dat geval is het aan te raden om een aparte duur van de verwerkersovereenkomst af te spreken.

12.2 Verwerkingsverantwoordelijke is gerechtigd de Verwerkersovereenkomst te ontbinden, indien Verwerker niet voldoet of niet langer kan voldoen aan de Verwerkersovereenkomst en/of de AVG en/of andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens en Verwerker in verzuim is, zonder dat Verwerker aanspraak maakt op enige schadevergoeding. Bij de ontbinding neemt Verwerkingsverantwoordelijke een redelijke opzegtermijn in acht, tenzij de omstandigheden onmiddellijke ontbinding rechtvaardigen.
12.3 Binnen één (1) maand nadat de Overeenkomst eindigt, vernietigt en/of retourneert Verwerker alle Persoonsgegevens en/of draagt Verwerker deze over aan Verwerkingsverantwoordelijke en/of een andere door Verwerkingsverantwoordelijke aan te wijzen partij, naar gelang de keuze van Verwerkingsverantwoordelijke. Alle bestaande (overige) kopieën van Persoonsgegevens, zich al dan niet bevindende bij door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers, worden hierbij aantoonbaar permanent verwijderd, tenzij opslag van de Persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht.

Ingevolge de AVG zijn er bij het beëindigen van de verwerkersovereenkomst twee mogelijkheden:

1. De (persoons)gegevens die zijn verwerkt worden door de leverancier vernietigd; of
2. De (persoons)gegevens die zijn verwerkt worden door de leverancier teruggegeven aan de instelling en bestaande kopieën worden verwijderd.

Voorgaande naar keuze van de instelling. Elke andere mogelijkheid biedt geen passende bescherming voor de (persoons)gegevens. Een uitzondering geldt als de leverancier onder de wet verplicht is bepaalde persoonsgegevens te bewaren.

Wet- en regelgeving:
- Artikel 28 lid 3 onder g AVG

12.4 Verwerker bevestigt op verzoek van Verwerkingsverantwoordelijke Schriftelijk dat Verwerker aan alle verplichtingen uit artikel 12.3 heeft voldaan.

12.5 Verwerker draagt de kosten voor vernietiging, retournering en/of overdracht van de Persoonsgegevens. Verwerkingsverantwoordelijke kan nadere eisen stellen aan de wijze van vernietiging, retournering en/of overdracht van de Persoonsgegevens, waaronder eisen aan het bestandsformaat. Bij de overdracht van Persoonsgegevens wordt uitgegaan van een open bestandsformaat. Partijen zullen in overleg een redelijke verdeling van eventuele extra kosten voor de nadere eisen bepalen.

12.6 Verplichtingen uit de Verwerkersovereenkomst die naar hun aard bestemd zijn om na beëindiging van de Verwerkersovereenkomst voort te duren, blijven na beëindiging van de Verwerkersovereenkomst voortduren.

ARTIKEL 13. TOEPASSELIJK RECHT EN GESCHILLENBESLECHTING

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

13.2 Alle geschillen, die tussen Partijen ontstaan in verband met de Verwerkersovereenkomst, zullen worden voorgelegd aan de bevoegde rechter in de plaats waar Verwerkingsverantwoordelijke gevestigd is.

ALDUS OVEREENGEKOMEN DOOR PARTIJEN:

[NAAM VERWERKINGSVERANTWOORDELIJKE]	**[NAAM VERWERKER]**
_____/_____/_____	_____/_____/_____
Datum	*Datum*
_____	_____
Naam	*Naam*
_____	_____
Handtekening	*Handtekening*

<u>Bijlage A</u>: Specificatie van de Verwerking van Persoonsgegevens

Versienummer XX, Datum laatste aanpassing: XX-XX-XX

NB. Indien Verwerker meerdere (optionele) Diensten aanbiedt aan Verwerkingsverantwoordelijke, is het mogelijk de informatie op te nemen in separate Bijlage(n), die als volgt genummerd worden: "<u>Bijlage A1</u>", "<u>Bijlage A2</u>", etc.
Deze Bijlagen dienen aan de Verwerkersovereenkomst te worden gehecht.

Zie de infographic 'De AVG in een notendop' die is gepubliceerd door de Autoriteit Persoonsgegevens als praktisch hulpmiddel voor het invullen van deze bijlage.

Wet- en regelgeving:
- Artikel 28 lid 3 en 9 AVG

Omschrijving van de Verwerking

Neem hier de naam van de dienst op. Bijvoorbeeld: 'salarisverwerking'.

Doeleinden van de Verwerking (*in te vullen door Verwerkingsverantwoordelijke*)

Schrijf hier zo concreet mogelijk het doel van de verwerking op. Denk hierbij aan het verwerken van sollicitaties, personeelsadministratie, salarisadministratie, pensioen of het vastleggen van inschrijvingsgeld voor een onderwijsinstelling.

Categorieën Betrokkenen (*in te vullen door Verwerkingsverantwoordelijke*)

Een betrokkene is degene over wie de persoonsgegevens gaan. Er kunnen verschillende categorieën betrokkenen zijn. Denk hierbij aan bijvoorbeeld studenten, medewerkers of contactpersonen.

(categorieën) Persoonsgegevens (*in te vullen door Verwerkingsverantwoordelijke*)

Het is naar eigen inzicht hoe gespecificeerd de persoonsgegevens worden opgeschreven. Het moet in ieder geval voor eenieder duidelijk zijn om welk soort persoonsgegevens het gaat. Bijvoorbeeld om naam, adres, telefoonnummer, maar denk ook aan loggegevens of tentamencijfers. Bekijk alle persoonsgegevens die in die dienst voorkomen.

Raadpleeg voor meer informatie de website van de Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens.

Frequentie verrichten van audit (*in te vullen door Verwerkingsverantwoordelijke*)

De frequentie van de audit is afhankelijk van het soort persoonsgegevens dat wordt verwerkt. Zie de toelichting bij artikel 6 van de verwerkersovereenkomst.

Bewaartermijn van de Persoonsgegevens of de criteria om die vast te stellen (*enkel invullen indien van toepassing)* (*in te vullen door Verwerkingsverantwoordelijke*)

Een belangrijk uitgangspunt van de AVG is 'opslagbeperking'. Dit houdt in dat persoonsgegevens niet langer bewaard worden dan noodzakelijk is voor de verwerking.

Sommige persoonsgegevens worden verwerkt zolang de dienst wordt afgenomen, in welk geval er afspraken worden gemaakt over overdracht of verwijdering van de gegevens zodra de dienst niet langer wordt gebruikt. Maar er zijn ook persoonsgegevens waarvoor het niet noodzakelijk is gedurende het gebruik van de dienst deze steeds te blijven bewaren. Denk hierbij aan het opslaan van back-ups en logging. De instelling en leverancier spreken hier af hoelang deze persoonsgegevens bewaard worden.

Wet- en regelgeving:

- Artikel 5 lid 1 sub e AVG

Categorieën Medewerkers

Categorieën Medewerkers (functierollen/functiegroepen) van Verwerker die Persoonsgegevens Verwerken	(categorie) Persoonsgegevens die door Medewerkers worden verwerkt	Soort Verwerking	Land van Verwerking

Hierboven worden de volgende punten beantwoord:

- Welke groepen medewerkers bij de persoonsgegevens kunnen. Denk aan beheerders, helpdeskmedewerkers etc.
- Om welke persoonsgegevens het gaat.
- Wat zij met deze persoonsgegevens kunnen (de soort verwerking): bijvoorbeeld lezen, bewerken of verwijderen.
- En in welk land de verwerking plaats vindt.

Sub-verwerkers

Verwerkingsverantwoordelijke heeft Verwerker [*aankruisen wat van toepassing is door Verwerkingsverantwoordelijke*]:

□ Algemene toestemming gegeven voor het inschakelen van Sub-verwerkers.

□ Specifieke toestemming gegeven voor het inschakelen van de hierna opgenomen Sub-verwerkers (*in te vullen door Verwerkingsverantwoordelijke*).

De door Verwerker ingeschakelde Sub-verwerkers zijn:

Sub-verwerker die door Verwerker wordt ingeschakeld voor het Verwerken van Persoonsgegevens	(categorie) Persoonsgegevens die Sub-verwerker verwerkt	Soort Verwerking	Land van Verwerking	Vestigingsland Sub-verwerker

Artikel 4.3 van de verwerkersovereenkomst geeft aan dat de instelling vooraf schriftelijke toestemming moet geven aan de leverancier als zij een sub-verwerker wil inschakelen. Dit kan zowel algemene als specifieke toestemming zijn. Kruis hierboven aan wat van toepassing is.

Het bovenstaande schema dient ingevuld te worden. De volgende vragen worden daar beantwoord:

- Welke sub-verwerkers (hulpleveranciers) de leverancier gaat inschakelen bij het leveren van de dienst?
- De persoonsgegevens waar de sub-verwerker toegang toe krijgt.
- Om wat voor dienstverlening van de sub-verwerker het gaat (bijvoorbeeld beheer of hosting).
- Het land waar de gegevensverwerking plaatsvindt. Als dit buiten de EER is moet er worden gekeken of er sprake is van een van de uitzonderingen uit artikel 8.1 van de verwerkersovereenkomst. Zie voor een verdere uitleg de uitwerking bij artikel 8.1.
- Het vestigingsland van de sub-verwerker. Indien de verwerking zelf binnen de EER plaatsvindt, maar het bedrijf waar je als instelling de overeenkomst mee sluit is gevestigd in een land buiten de EER, zal er alsnog moeten worden gekeken of er sprake is van een van de uitzondering uit artikel 8.1 van de verwerkersovereenkomst.

Doorgiften buiten de Europese Economische Ruimte

Verwerkingsverantwoordelijke heeft Verwerker specifieke toestemming gegeven voor de hierna opgenomen doorgiften aan derde landen of internationale organisaties (*in te vullen door Verwerkingsverantwoordelijke*).

Zie de toelichting bij artikel 8 van de verwerkersovereenkomst voor doorgifte van gegevens.

Beschrijving doorgifte	**Entiteit die de Persoonsgegevens doorgeeft + land**	**Entiteit die de Persoonsgegevens ontvangt + land**	**Doorgifte-mechanisme**	**Extra getroffen waarborgen voor doorgifte buiten de EER**

Contactgegevens

Algemene contactgegevens	**Naam**	**Functie**	**E-mail adres**	**Telefoonnummer**
Verwerkings-verantwoordelijke (*in te vullen door Verwerkings-verantwoordelijke)*				

Verwerker				

Contactgegevens bij Inbreuk in verband met Persoonsgegevens	**Naam**	**Functie**	**E-mail adres**	**Telefoonnummer**
Verwerkings-verantwoordelijke (*in te vullen door Verwerkings-verantwoordelijke)*				
Verwerker				

Vul hierboven in met wie de verwerker contact moet opnemen in het geval van een mogelijk datalek. Vul zo veel mogelijk gegevens in, zodat de verwerker altijd een manier heeft om het datalek zo snel mogelijk te melden. In sommige gevallen zal de contactpersoon de Functionaris Gegevensbescherming zijn, maar dit hoeft niet altijd zo te zijn. In dat geval kan ervoor worden gekozen nog een tabel toe te voegen waarin de contactgegevens van de Functionaris Gegevensbescherming worden opgenomen.

Bijlage B: **Beveiligingsmaatregelen**

De AVG stelt dat de verwerker 'passende technische en organisatorische beveiligingsmaatregelen' moet treffen om persoonsgegevens te beveiligen. Een certificering kan helpen aantonen dat een verwerker 'passende technische en organisatorische maatregelen' heeft getroffen om te voldoen aan de AVG.

Bij de uitwerking van de getroffen beveiligingsmaatregelen in deze bijlage kan de instelling bijvoorbeeld vragen om een ISO-certificering of om het beveiligingsbeleid van de leverancier.

Voor meer informatie over passende beveiligingsmaatregelen zie artikel 5 van de verwerkersovereenkomst en de Handreiking Beveiligingsmaatregelen, Bijlage C Juridisch Normenkader:
https://www.surf.nl/binaries/content/assets/surf/nl/2018/jnk-2018/surf_c-handreiking-beveiligingsmaatregelen---bijlage-c---versie-mei-2018.pdf.

Versienummer XX, Datum laatste aanpassing: XX-XX-XX

Uitwerking van de door Verwerker getroffen beveiligingsmaatregelen:

Certificaten waarover Verwerker beschikt:

Certificaten	Organisatieonderdeel / dienst waarop certificaat betrekking heeft	Geldigheidsduur certificaat	Verklaring van toepasselijkheid

Als instelling is het belangrijk om niet alleen te vragen naar een (ISO-)certificaat, maar tevens naar de Verklaring van Toepasselijkheid. Het certificaat geeft weer wat er tijdens de audit is gecontroleerd. Bij de ISO-certificeringen is het echter mogelijk om beheersmaatregelen uit het zogenaamde specifieke deel van de ISO-certificering, op ‘niet van toepassing’ te zetten. Deze maatregelen worden dan ook niet geaudit. In dat geval is dat deel van de norm dus niet geïmplementeerd bij de dienstverlening van leverancier. Daarom is het van belang om het certificaat zelf op te vragen om de scope te kunnen inzien en tevens de Verklaring van Toepasselijkheid te vragen, waarin wordt uitgewerkt welke beheersmaatregelen wel en niet van toepassing zijn verklaard voor de certificering.