Instructie bij Model Verwerkersovereenkomst

Juridisch Normenkader (Cloud)services, Bijlage B

Utrecht, maart 2018
Versienummer: 2.0

Colofon

Instructie bij Model Vewerkersovereenkomst
SURF Juridisch Normenkader (Cloud)services, Bijlage B

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

info@surf.nl
www.surf.nl

Maart 2018

SURF is de ICT-samenwerkingsorganisatie van het Nederlandse hoger onderwijs en onderzoek.
Deze publicatie is digitaal beschikbaar via de website van SURF: www.surf.nl/publicaties

Inleiding

Dit is een instructie en uitleg die hoort bij de Model Verwerkersovereenkomst, versie 2.0 (oktober 2017) 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 dat dit, worden doorgaans opgenomen in de hoofdovereenkomst. Denk daarbij aan intellectueel eigendom (dat kan ook gaan om data die geen persoonsgegevens zijn) en vertrouwelijkheid (data die geen persoonsgegevens zijn kunnen ook vertrouwelijk zijn, denk aan bedrijfsgevoelige informatie). Standaardbepalingen om deze onderwerpen in de hoofdovereenkomst te regelen zijn te vinden in de notitie van het SURF Juridisch Normenkader (Cloud)services.

Dit document blijft 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 bepaling 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. Deze handleiding vervangt de oude 'Handleiding Wbp'.

Beleidsregels voor toepassing van artikel 34a van de Wbp, Autoriteit Persoonsgegevens, december 2015
Beleidsregels rond de meldplicht datalekken, te vinden op de website van de Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/melden/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 oktober 2016. Het document is te vinden op de website van SURF:
https://www.surf.nl/kennisbank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html

Handreiking Auditverplichting, Bijlage D Juridisch Normenkader
Leidraad voor de invulling van de auditverplichting uit de bewerkersovereenkomst, horend bij het SURF Juridisch Normenkader (Cloud)services. Versie oktober 2016. Het document is te vinden op de website van SURF: https://www.surf.nl/kennisbank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html

*: Op het moment van publiceren van deze Instructie, is het Wetsvoorstel voor de Uitvoeringswet nog niet definitief. De verwachting is echter dat deze wet per 25 mei 2018 in Nederland van toepassing zal zijn."

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 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;

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 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.

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.

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 Betrokkene: de geïdentificeerde of identificeerbare natuurlijke persoon op wie de Persoonsgegevens betrekking hebben, zoals bedoeld in artikel 4 onder 1) AVG.

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

1.4 Bijzondere categorieën Persoonsgegevens: Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, zoals bedoeld in artikel 9 AVG.

1.5 Derde: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de Betrokkene, noch de Verwerkingsverantwoordelijke, noch de Verwerker, noch de personen die onder rechtstreeks gezag van de Verwerkingsverantwoordelijke of de Verwerker gemachtigd zijn om Persoonsgegevens te verwerken, zoals bedoeld in artikel 4 onder 10) AVG.

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

1.7 Inbreuk in verband met Persoonsgegevens: een (vermoeden van een) inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte Persoonsgegevens, zoals bedoeld in artikel 4 onder 12) AVG.

1.8 Medewerker: de door Verwerker ingeschakelde werknemers en andere personen waarvan de werkzaamheden onder zijn verantwoordelijkheid vallen en die worden ingeschakeld door Verwerker ter uitvoering van de Overeenkomst.

1.9 Ontvanger: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een Derde, aan wie/waaraan de Persoonsgegevens worden verstrekt, zoals bedoeld in artikel 4 onder 9) AVG.

1.10 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.

1.11 Persoonsgegeven: alle informatie over een Betrokkene; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van

een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon, zoals bedoeld in artikel 4 onder 1) AVG.

1.12 PIA: de gegevensbeschermingseffectbeoordeling (privacy impact assessment) 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.

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

1.14 Sub-verwerker: een andere verwerker, waaronder maar niet beperkt tot groepsmaatschappijen, zustermaatschappijen, dochtermaatschappijen en hulpleveranciers, die Verwerker inschakelt om voor rekening van de Verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten.

1.15 Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens: de toepasselijke wet- en regelgeving en/of (nadere) verdragen, verordeningen, richtlijnen, besluiten, beleidsregels, instructies en/of aanbevelingen van een bevoegde overheidsinstantie betreffende de Verwerking van Persoonsgegevens, tevens omvattende toekomstige wijziging hiervan en/of aanvulling hierop, inclusief lidstaatrechtelijke uitvoeringswetten van de AVG en de Telecommunicatiewet.

1.16 Toezichthoudende autoriteit: één of meer onafhankelijke overheidsinstanties die verantwoordelijk is of zijn voor het toezicht op de toepassing van de AVG, teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met de Verwerking van hun Persoonsgegevens te beschermen en het vrije verkeer van Persoonsgegevens binnen de Unie te vergemakkelijken, zoals bedoeld in artikel 4 onder 21) en artikel 51 AVG. In Nederland is dit de Autoriteit Persoonsgegevens.

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

1.18 Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens, zoals bedoeld in artikel 4 onder 2) AVG.

Alle handelingen die met persoonsgegevens worden verricht zijn aan te merken als het verwerken hiervan. Hier valt ook enkel het opslaan, hosten, doorgeven of bijvoorbeeld vernietigen van persoonsgegevens onder.

Wet- en regelgeving:
- Artikel 4 lid 2 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 2.1 opgenomen dat de verwerkersovereenkomst voor de hoofdovereenkomst gaat. Het is belangrijk dat er in de andere overeenkomsten 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 heeft als verwerkingsverantwoordelijke een verplichting onder de AVG om te zorgen dat de leverancier in staat is om diens verplichtingen uit de AVG na te komen. 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. De instructies van Verwerkingsverantwoordelijke zijn nader omschreven in de Verwerkersovereenkomst en de Overeenkomst. Verwerkingsverantwoordelijke kan naar redelijkheid Schriftelijk aanvullende of afwijkende instructies geven.

2.4 Verwerker verwerkt de Persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke en op basis van de instructies van Verwerkingsverantwoordelijke. 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 reclamedoeleinden) 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.

2.5 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 AVG.

2.6 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. VERWERKING VAN PERSOONSGEGEVENS

3.1 Voorafgaand aan het sluiten van de Verwerkersovereenkomst informeert Verwerker Verwerkingsverantwoordelijke in Bijlage A volledig en naar waarheid over de Verwerkingen die Verwerker ter uitvoering van de Overeenkomst uitvoert, tenzij in Bijlage A is opgenomen dat Verwerkingsverantwoordelijke de betreffende informatie in deze Bijlage opneemt. 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.

ARTIKEL 4. VERLENEN VAN BIJSTAND EN MEDEWERKING

4.1 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 Verwerkingsverantwoordelijke in ieder geval bijstand met betrekking tot:

(i) De beveiliging van Persoonsgegevens;

(ii) Het uitvoeren van controles en audits;

(iii) Het uitvoeren van PIA'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 een gegevensbeschermingseffectbeoordeling 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.

4.2 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:

4.2.1 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), en
- het recht tot data-export/dataportabiliteit (artikel 19 AVG);
- het recht op bezwaar (artikel 21 AVG);
- 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.

4.2.2 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. Dergelijke verzoeken dienen eerst op rechtmatigheid getoetst te worden door de instelling. In uitzonderingsgevallen kan de instelling een andersluidende instructie geven aan de leverancier.

De betreffende rechten van betrokkenen zijn te vinden in de artikelen 13 t/m 22 AVG.

4.2.3 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 4.2.3 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. In deze Code of Conduct staat een dergelijke bepaling zoals geformuleerd in 4.2.3. In artikel 4.2.3 is echter expliciet opgenomen dat een dergelijke verplichting om de betrokkene te informeren enkel op verzoek van de instelling kan. Deze verplichting komt niet in de plaats van de plichten die de instelling zelf heeft op grond van de AVG.

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

De Code of Conduct is te vinden op de website van GÉANT:

http://geant3plus.archive.geant.net/uri/dataprotection-code-of-conduct/Pages/default.aspx.

4.3 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:

4.3.1 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 dergelijke verzoeken of bevelen te zijn.

4.3.2 Indien het Verwerker wettelijk is verboden om te voldoen aan zijn verplichtingen op grond van artikel 4.3.1, behartigt Verwerker de redelijke belangen van Verwerkingsverantwoordelijke. Hieronder wordt in ieder geval verstaan:

4.3.2.1 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 4.3.1 te voldoen.

4.3.2.2 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.

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

4.3.2.4 Verwerker onderzoekt indien sprake is van doorgifte in de zin van artikel 9 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 het derde lid. In die gevallen dient de instelling alsnog de beveiliging van de gegevens te waarborgen. 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 44-46 AVG gaan over doorgifte van gegevens naar derde landen. Dit is alleen toegestaan als er sprake is van een van de in die artikelen genoemde uitzonderingen. Zie artikel 9 van dit Instructiemodel voor een verdere toelichting van deze artikelen.

ARTIKEL 5. TOEGANG TOT PERSOONSGEGEVENS

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

5.2 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 dient in de verwerkersovereenkomst te worden vastgelegd welke medewerkers (functionarissen) of welke groepen medewerkers welke verwerkingen 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 Strafrecht.

Wet- en regelgeving:
- Artikel 28 lid 3 onder b) en artikel 32 lid 4 AVG.
- Artikel 29 AVG.

5.3 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 welk soort toestemming wordt gekozen.

Wet- en regelgeving:
- Artikel 28 lid 2 AVG.

5.4 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), Schriftelijk in, waarbij de Verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken. Partijen treden hierop in onderhandeling.

Indien de instelling het niet eens is met de inschakeling van een bepaalde sub-verwerker, heeft hij 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 te allen tijde toezicht moet kunnen houden op de verwerking.

Wet- en regelgeving:
- Artikel 28 lid 2 AVG.

5.5. De algemene of specifieke toestemming van Verwerkingsverantwoordelijke voor het inschakelen Sub-verwerkers laat de verplichtingen voor Verwerker voortvloeiende uit de Verwerkersovereenkomst, waaronder maar niet beperkt tot artikel 9, 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.

5.6 Verwerker verstrekt op eerste verzoek van Verwerkingsverantwoordelijke een overzicht van de door Verwerker ingeschakelde Sub-verwerkers aan Verwerkingsverantwoordelijke.

Op grond van de AVG is de instelling verplicht om toe te zien op de verwerking van persoonsgegevens door leveranciers en eventuele sub-verwerkers. Om aan deze verplichting te kunnen voldoen, is de leverancier gehouden om op verzoek van de instelling zo spoedig mogelijk een overzicht van de ingeschakelde sub-verwerkers te geven.

Wet- en regelgeving:
- Artikel 28 lid 1 en 2 AVG.

5.7 Verwerker legt de in de Verwerkersovereenkomst opgenomen verplichtingen op aan de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers. Verwerker draagt er zorg voor dat de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers, de in de Verwerkersovereenkomst opgenomen verplichtingen naleven door middel van een Schriftelijke overeenkomst.

5.8 Verwerker brengt Verwerkingsverantwoordelijke onverwijld op de hoogte indien Verwerker en/of door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers, in strijd handelen met de Verwerkersovereenkomst en/of de met Verwerker gesloten Schriftelijke overeenkomst zoals bedoeld in artikel 5.7.

5.9 Verwerker verstrekt op verzoek van Verwerkingsverantwoordelijke een afschrift van de Schriftelijke overeenkomst tussen Verwerker en de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers.

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 een afschrift van de overeenkomst met de sub-verwerker te verstrekken.

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

5.10 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, 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 6. BEVEILIGING

6.1 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 verwerkingsverantwoordelijke 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:

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

6.2 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.

6.3 Verwerker legt zijn beveiligingsbeleid Schriftelijk vast. Op verzoek van Verwerkingsverantwoordelijke verschaft Verwerker inzage in het beveiligingsbeleid van 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 schriftelijke informatie over de informatiebeveiliging te verstrekken.

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

6.4 Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 AVG of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 AVG kan worden gebruikt als element om aan te tonen dat de in dit artikel bedoelde vereisten worden nageleefd.

Brancheorganisaties kunnen bij wijze van zelfregulering specifieke uitwerkingen van de AVG opstellen middels gedragscodes, en deze door de toezichthouder laten goedkeuren.

Bij certificering kan een verwerkingsverantwoordelijke of een verwerker via een speciale procedure (het certificeringsmechanisme) een proces van verwerking, een middel voor verwerking of een daarbij ondersteunend middel zoals een beveiliging laten toetsen. Indien hieraan is voldaan, kan men een zegel of merkteken voeren.

Wet- en regelgeving:
- Artikel 32 lid 3 AVG.

ARTIKEL 7. AUDIT

7.1 Verwerker is verplicht 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 Overeenkomst, 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.

Bovendien is de leverancier verplicht om mee te werken aan audits ter verificatie dat hij voldoet aan de verplichtingen uit deze verwerkersovereenkomst en meer algemeen de AVG.

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

7.2 Verwerker verricht tenminste een keer per twee jaar een periodieke audit, zoals bedoeld in artikel 7.1. Indien Bijzondere categorieën Persoonsgegevens worden verwerkt, verricht Verwerker tenminste eenmaal per jaar een periodieke audit zoals bedoeld in artikel 7.1.

7.3 Verwerker is enkel niet gehouden tot het verrichten van een periodieke audit zoals bedoeld in artikel 7.1, indien Verwerker uitsluitend Persoonsgegevens verwerkt met een laag risico en uitdrukkelijk in Bijlage A is opgenomen dat Verwerker niet gehouden is tot het verrichten van een periodieke audit. Verwerkingsverantwoordelijke stelt vast of er sprake is van een laag risico.

Afhankelijk van de risicoklasse dient de dienstverlening en de beveiliging van de leverancier door de instelling te worden gecontroleerd. Dit kan worden gedaan door een periodieke controle door een onafhankelijke deskundige. Hoe vaak de leverancier verplicht is een audit te doen hangt af van het soort persoonsgegevens.

Er zijn drie soorten risicoklassen:

- Risicoklasse 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.*
- Risicoklasse 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, financiële gegevens of locatiegegevens. *De audit verplichting is 1 keer per 2 jaar.*
- Risicoklasse Hoog: hier gaat het in ieder geval om persoonsgegevens die vallen in de categorie 'Bijzondere Persoonsgegevens' (artikel 9 AVG), waar onder andere politieke opvattingen, gegevens waaruit ras of etnische afkomst blijken, genetische en biometrische gegevens onder vallen. Tevens vallen hier strafrechtelijke gegevens en het nationale identificatienummer (BSN/onderwijsnummer) onder. *De auditverplichting is jaarlijks.*

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.

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:

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.

7.4 Verwerker is verplicht de bevindingen van de onafhankelijke, externe deskundige, op verzoek aan Verwerkingsverantwoordelijke ter beschikking te stellen in de vorm van een verklaring, waarin de deskundige 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.

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 onafhankelijke, 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 naar hoeft te (laten) doen.

7.5 Verwerkingsverantwoordelijke heeft het recht om op zijn verzoek een audit te laten uitvoeren door een door Verwerkingsverantwoordelijke gemachtigde (rechts)persoon, ten aanzien van de organisatie van Verwerker, teneinde aan te tonen dat Verwerker aan het bepaalde in de Overeenkomst, de Verwerkersovereenkomst, de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet.

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.

7.6 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 Overeenkomst en/of de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens niet is nagekomen. Deze bepaling laat de overige rechten van Verwerkingsverantwoordelijke, waaronder het recht op schadevergoeding, onverlet.

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 die een direct verband heeft met het vermoeden van niet nakoming door Verwerker. De scope van dit onderzoek is dus beperkt tot de afspraken waarvan een instelling het redelijke vermoeden heeft dat deze zijn geschonden.

De uitvoering van dit onderzoek wordt in eerste instantie bekostigd door de Instelling. 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.

7.7 Indien tijdens een audit wordt vastgesteld dat Verwerker niet aan het bepaalde in de Overeenkomst en/of 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 8. INBREUK IN VERBAND MET PERSOONSGEGEVENS

8.1 Verwerker informeert Verwerkingsverantwoordelijke zonder onredelijke vertraging en uiterlijk binnen 24 uur na kennisneming, over een Inbreuk in verband met Persoonsgegevens of een redelijk vermoeden van 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 hetgeen is opgenomen in Bijlage C. Verwerker garandeert dat de verstrekte informatie volledig, correct en accuraat is.

Volgens de AVG moet de instelling datalekken die vallen onder de meldplicht binnen 72 uur 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 bepaalde datalek gemeld dient te worden of niet, is het belangrijk dat de leverancier alle inbreuken of redelijke vermoedens hiervan 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.

In Bijlage C staat de informatie opgesomd die de leverancier moet leveren aan de instelling. Dit is gebaseerd op het formulier datalekken van de Autoriteit Persoonsgegevens.

In Bijlage A kan worden aangegeven bij welk persoon of welke afdeling de leverancier het mogelijke datalek moet melden bij de instelling.

Wet- en regelgeving:
- Artikel 28 lid 3 onder f) en artikel 33 AVG.
- Beleidsregels voor toepassing van artikel 34a van de Wbp, Autoriteit Persoonsgegevens, december 2015.

8.2 Indien en voor zover het voor Verwerker niet mogelijk is om alle informatie uit Bijlage C gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging en uiterlijk binnen 24 uur na het ontdekken, in stappen worden verstrekt aan Verwerkingsverantwoordelijke.

Wet- en regelgeving:
- Artikel 33 lid 4 AVG.

8.3 Verwerker heeft adequaat beleid en adequate procedures ingericht om Inbreuken in verband met Persoonsgegevens in een zo vroeg mogelijk stadium te detecteren, Verwerkingsverantwoordelijke hierover uiterlijk binnen 24 uur te informeren, hierop adequaat en onmiddellijk te reageren, (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.

8.4 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. Dit houdt in dat ook de leverancier een dergelijk register moet bijhouden en deze aan de instelling dient te verschaffen op verzoek van de instelling.

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

ARTIKEL 9. DOORGIFTE VAN PERSOONSGEGEVENS

9.1 Persoonsgegevens mogen enkel worden doorgegeven aan derde landen of internationale organisaties indien sprake is van een passend beschermingsniveau en Verwerkingsverantwoordelijke hiervoor specifieke Schriftelijke toestemming heeft verleend. Deze specifieke Schriftelijke toestemming is slechts verleend indien dit is opgenomen 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.

9.2 Verwerkingsverantwoordelijke kan aan de Schriftelijke toestemming, zoals bedoeld in artikel 9.1, nadere voorwaarden verbinden, waaronder maar niet beperkt tot het aantonen dat aan de vereisten zoals opgenomen in artikel 9.3 is voldaan.

9.3 Verwerkingsverantwoordelijke kan Verwerker slechts toestemming verlenen voor een doorgifte van Persoonsgegevens aan derde landen of internationale organisaties indien, ofwel:

(i) Een adequaatheidsbesluit overeenkomstig artikel 45 lid 3 AVG is genomen ten aanzien van het betreffende derde land of de betreffende internationale organisatie; ofwel

(ii) Passende waarborgen overeenkomstig artikel 46 AVG met inbegrip van bindende voorschriften zoals bedoeld in artikel 47 AVG, zijn getroffen ten aanzien van het betreffende derde land of de betreffende internationale organisatie; ofwel

(iii) Aan één van de specifieke voorwaarden uit artikel 49 lid 1 AVG is voldaan ten aanzien van het betreffende derde land of de betreffende internationale organisatie.

Ingevolge de AVG moeten er in de verwerkersovereenkomst afspraken zijn gemaakt omtrent doorgifte van persoonsgegevens naar derde landen.

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 (Europees Economische Ruimte: alle landen van de EU plus Noorwegen, Liechtenstein en IJsland).

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.[1] Meer over verwerking in de VS en de huidige stand van zaken rond het Privacy Shield is te vinden op de website van de Autoriteit Persoonsgegevens:

[1] Op het moment van publiceren van deze Handreiking, wordt het EU-VS Privacyshield nog beschouwd als zijnde een ‘adequaat beschermingsniveau’ in de zin van artikel 45 AVG. Wegens een 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.

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal gegevensverkeer/doorgifte-binnen-en-buiten-de-eu.

2. Indien sprake is van een van de 'passende waarborgen' of Binding Corporate Rules (artikel 46 en 47 AVG). Dit betreffen de volgende maatregelen:

- Binding Corporate Rules;
- Modelcontract van de Europese Commissie;
- Modelcontract van de Autoriteit Persoonsgegevens;
- een zelf opgestelde en door de Autoriteit Persoonsgegevens goedgekeurde overeenkomst;
- gedragscode;
- certificering.

3. Indien sprake is van een van de specifieke situaties uit artikel 49 lid 1 AVG. Dit betreffen:
- uitdrukkelijke toestemming van de betrokkene;
- als de doorgifte noodzakelijk is voor het aangaan of uitvoeren van een overeenkomst (restrictief uitgelegd);
- als doorgifte noodzakelijk is voor gewichtige redenen van algemeen belang;
- als doorgifte noodzakelijk is voor het instellen, uitoefenen of onderbouwen van een rechtsvordering;
- als doorgifte noodzakelijk is voor een vitaal belang van een persoon;
- voor een bij wet ingesteld register;
- 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.

ARTIKEL 10. VERTROUWELIJKHEID VAN PERSOONSGEGEVENS

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

10.2 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 dwingendrechtelijk wettelijk voorschrift of rechterlijke uitspraak Partijen tot bekendmaking en/of verstrekking van die Persoonsgegevens verplicht, waarbij Partijen eerst de andere Partij hiervan op de hoogte stellen;

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

10.3 Overtreding van artikel 10.1 en/of artikel 10.2 wordt beschouwd als een Inbreuk in verband met Persoonsgegevens.

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

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 (het voorstel voor) de Nederlandse Wet bescherming bedrijfsgeheimen.

ARTIKEL 11. AANSPRAKELIJKHEID EN VRIJWARING

11.1 Verwerker is aansprakelijk voor alle schade die voortvloeit uit of verband houdt met het niet nakomen van de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

Op grond van het Burgerlijk Wetboek is een partij die tekortschiet in de nakoming van een overeenkomst, aansprakelijk voor de schade die daaruit voortvloeit.

Wet- en regelgeving:
- Artikel 6:74 BW.

11.2 Verwerker vrijwaart Verwerkingsverantwoordelijke voor alle aanspraken, boeten en/of maatregelen van derden, daaronder begrepen Betrokkenen en de Toezichthoudende autoriteit, die jegens Verwerkingsverantwoordelijke worden ingesteld of opgelegd wegens een schending van de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens door Verwerker en/of door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers.

Wanneer een derde (bijvoorbeeld een betrokkene) de instelling aanspreekt op een schending van de AVG (of andere wet- en regelgeving m.b.t. persoonsgegevens) en de schending is te wijten aan de leverancier of een derde die door de leverancier is ingeschakeld dan vrijwaart de leverancier de instelling voor deze aanspraak.

Wanneer de leverancier een derde partij inschakelt voor de verwerking van persoonsgegevens betekent dat niet dat de leverancier zich niet meer hoeft te houden aan de verplichting ten aanzien van de persoonsgegevens. Bovendien is de leverancier ingevolgde de AVG volledig aansprakelijk voor het nakomen van de verplichtingen van de derde partij.

Artikel 82 leden 1, 2 en 4 AVG stellen 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.

Wet- en regelgeving:
- Artikel 28 lid 4 AVG.

11.3 Verwerker draagt zorg voor afdoende dekking van de aansprakelijkheid door middel van een aansprakelijkheidsverzekering. Op verzoek van Verwerkingsverantwoordelijke geeft Verwerker Verwerkingsverantwoordelijke inzage in (de polis van) deze aansprakelijkheidsverzekering van Verwerker.

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 te letten op de volgende punten:

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

ARTIKEL 12. WIJZIGING

12.1 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. 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 aan derde landen en/of internationale organisaties.

12.2 Indien een wijziging met betrekking tot de Verwerking van Persoonsgegevens of een audit daartoe aanleiding geeft, treden Partijen op eerste verzoek van Verwerkingsverantwoordelijke in overleg over het wijzigen van de Verwerkersovereenkomst.

12.3 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 tot gevolg heeft, indien Verwerkingsverantwoordelijke daaraan voorafgaand Schriftelijk toestemming voor deze wijziging(en) heeft gegeven.

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. Daartoe is de informatieplicht van dit artikel opgenomen.

Wet- en regelgeving:
- Artikel 28 lid 1 AVG.

12.4 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.

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

ARTIKEL 13. DUUR EN BEËINDIGING

13.1 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 beëindiging 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.

13.2 Verwerkingsverantwoordelijke is gerechtigd de Verwerkersovereenkomst op te zeggen, 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, zonder dat Verwerker aanspraak maakt op enige schadevergoeding. Bij de opzegging neemt Verwerkingsverantwoordelijke een redelijke opzegtermijn in acht, tenzij de omstandigheden onmiddellijke opzegging rechtvaardigen.

13.3 Binnen een 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.

13.4 Verwerker bevestigt op verzoek van Verwerkingsverantwoordelijke Schriftelijk dat Verwerker aan alle verplichtingen uit artikel 13.3 heeft voldaan.

13.5 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.

13.6 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.

Ingevolge de AVG zijn er bij het beëindigen van de overeenkomst 2 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.

ARTIKEL 14. TOEPASSELIJK RECHT EN GESCHILLENBESLECHTING

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

14.2 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 INSTELLING	**NAAM LEVERANCIER**
_____/_____/_____	_____/_____/_____
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), welke 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 lid 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 welke persoonsgegevens het gaat. Bijvoorbeeld om naam, adres, telefoonnummer, maar denk ook aan loggegevens of tentamencijfers. Bekijk alle persoonsgegevens die in die dienst voorkomen.

Meer over persoonsgegevens, zie 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 7 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 worden bewaard.

Wet- en regelgeving:
- Artikel 5 lid 1 onder 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

In de tabel 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*):

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

Artikel 5.3 van de verwerkersovereenkomst geeft aan dat de instelling vooraf schriftelijke toestemming moet geven aan de leverancier als hij een sub-verwerker wil inschakelen. Dit kan zowel algemene als specifieke toestemming zijn. Kruis hierboven aan wat van toepassing is.

Indien er sprake is van specifieke toestemming, dient het bovenstaande schema 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 9.3 van de verwerkersovereenkomst. Zie voor een verdere uitleg de uitwerking bij artikel 9.3 van deze verwerkersovereenkomst.
- 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 uitzonderingen uit artikel 9.3 van de verwerkersovereenkomst ter doorgifte van persoonsgegevens.

Doorgiften

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 9 van de verwerkersovereenkomst voor doorgifte van gegevens.

Beschrijving doorgifte	**Entiteit die de Persoonsgegevens doorgeeft + land**	**Entiteit die de Persoonsgegevens ontvangt + land**	**Doorgifte-mechanisme**

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 op moet nemen 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 FG zijn, maar dit hoeft niet altijd zo te zijn. In dat geval kan er voor worden gekozen nog een tabel toe te voegen waarin de contactgegevens van de FG worden opgenomen.

Bijlage B: **Beveiligingsmaatregelen**

De AVG stelt dat verwerkers ‘passende technische en organisatorische beveiligingsmaatregelen’ moeten 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 6 van de verwerkersovereenkomst en de Handreiking Beveiligingsmaatregelen, Bijlage C Juridisch Normenkader:

https://www.surf.nl/kennisbank/2013/surf-juridisch-normenkader-cloudservices.html

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 de 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.

Kwalificaties waaraan Verwerker voldoet:

Bijlage C: Informatie die moet worden verstrekt bij een Inbreuk in verband met Persoonsgegevens

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

In deze bijlage wordt vermeld welke informatie de verwerker moet verschaffen aan de instelling bij een datalek. De vragen zijn gebaseerd op de gegevens die moeten worden ingevuld als de instelling als verwerkingsverantwoordelijke een datalek moet melden aan de Autoriteit Persoonsgegevens.
Het formulier om een datalek te melden (waar deze bijlage op is gebaseerd) is te vinden op de website van de autoriteit:

https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0.

Deze bijlage hoeft, in tegenstelling tot bijlage A en B, niet verder te worden ingevuld. Wel dient bovenaan het versienummer van de bijlage te worden ingevuld en de datum van laatste aanpassing.

Contactgegevens melder

Naam, functie, emailadres, telefoonnummer.

Gegevens over de Inbreuk in verband met Persoonsgegevens (hierna: "Inbreuk")

- Geef een samenvatting van het incident waarbij de Inbreuk op de beveiliging van Persoonsgegevens zich heeft voorgedaan.
- Van hoeveel personen zijn Persoonsgegevens betrokken bij de Inbreuk?
  (Vul de aantallen in.)
  a) Minimaal: (vul aan)
  b) Maximaal: (vul aan)
- Omschrijf de groep mensen van wie Persoonsgegevens zijn betrokken (Categorieën Betrokkenen) bij de Inbreuk.
- Wanneer vond de Inbreuk plaats?
  (Kies een van de volgende opties en vul waar nodig aan)
  a) Op (datum)
  b) Tussen (begindatum periode) en (einddatum periode)
  c) Nog niet bekend
- Wat is de aard van de Inbreuk?
  (U kunt meerdere mogelijkheden aankruisen)
  a) Lezen (vertrouwelijkheid)
  b) Kopiëren
  c) Veranderen (integriteit)
  d) Verwijderen of vernietigen (beschikbaarheid)
  e) Diefstal

f) Nog niet bekend

- Om welk type Persoonsgegevens gaat het?
  (U kunt meerder mogelijkheden aankruisen)

  a) Naam -, adres - en woonplaatsgegevens

  b) Telefoonnummers

  c) E - mailadressen of andere adressen voor elektronische communicatie

  d) Toegangs - of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord of klantnummer)

  e) Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)

  f) Burgerservicenummer (BSN) of sofinummer

  g) Paspoortkopieën of kopieën van andere legitimatiebewijzen

  h) Geslacht, geboortedatum en/of leeftijd

  i) Bijzondere categorieën Persoonsgegevens (ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid)

  j) Overige gegevens, namelijk (vul aan)

- Welke gevolgen kan de Inbreuk hebben voor de persoonlijke levenssfeer van de Betrokkenen?
  (U kunt meerdere mogelijkheden aankruisen)

  a) Stigmatisering of uitsluiting

  b) Schade aan de gezondheid

  c) Blootstelling aan (identiteits)fraude

  d) Blootstelling aan spam of phishing

  e) Anders, namelijk (vul aan)

Vervolgacties naar aanleiding van het Inbreuk in verband met Persoonsgegevens

- Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

Technische beschermingsmaatregelen

- Zijn de Persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?
  (Kies een van de volgende opties en vul waar nodig aan)

  a) Ja

  b) Nee

  c) Deels, namelijk: (vul aan)

- Als de Persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd?
  (Beantwoord deze vraag als u bij de vorige vraag gekozen heeft voor optie a of optie c. Als u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.)

Internationale aspecten

- Heeft de Inbreuk betrekking op personen in andere EU-landen?
  (Kies een van de volgende opties)

  a) Ja

  b) Nee

  c) Nog niet bekend