

Verwerkersovereenkomst

Afnemer – Logius

Inzake MijnOverheid

Versie 1.4 – 20-06-2019

DE ONDERGETEKENDEN:

....., gevestigd in
....., te dezen rechtsgeldig vertegenwoordigd door
met als functie, hierna te noemen : "Afnemer"

en

De Staat der Nederlanden, te dezen rechtsgeldig vertegenwoordigd door de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, voor deze de Algemeen Directeur Logius, ir. Y.L. (Yvonne) van der Brugge-Wolring, namens deze de heer G. Gihaux, clustermanager Business/Relatie-Sourcing, hierbij domicilie kiezend aan de Wilhelmina van Pruisenweg 52 te 2595 AN Den Haag, hierna te noemen: "Logius"

Hierna ieder afzonderlijk aan te duiden als "Partij", of tezamen aangeduid als "Partijen",

OVERWEGENDE DAT:

- Afnemer en Logius een overeenkomst zijn aangegaan op grond waarvan Logius diensten levert aan de Afnemer;
- Door Afnemer, als 'verwerkingsverantwoordelijke' in de zin van de Algemene Verordening Gegevensbescherming¹, persoonsgegevens worden verwerkt;
- Logius, als 'verwerker' in de zin van de Algemene Verordening Gegevensbescherming, op grond van de door haar te leveren diensten te maken krijgt met deze persoonsgegevens;
- De reikwijdte van deze Verwerkersovereenkomst is dat Logius optreedt als verwerker van persoonsgegevens waarvoor Afnemer is aan te merken als 'verwerkingsverantwoordelijke' in de zin van de Algemene Verordening Gegevensbescherming;
- Afnemer en Logius in overeenstemming met de Algemene Verordening Gegevensbescherming, hun afspraken over de verwerking van persoonsgegevens wenselijk vast te leggen in deze Verwerkersovereenkomst.

VERKLAREN ALS VOLGT TE ZIJN OVEREENGEKOMEN:

Artikel 1. Definities

In deze Verwerkersovereenkomst hebben onderstaande definities de onderstaande betekenissen:

1.1. *Dienst(en)*: de door Logius aan Afnemer te leveren diensten zoals beschreven in

¹ 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).

Bijlage(n) bij deze Verwerkersovereenkomst.

- 1.2. *Persoonsgegevens*: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, voor zover dat gegeven in opdracht van de Afnemer wordt verwerkt.
- 1.3. *Functionaris Gegevensbescherming*: de door Afnemer benoemde functionaris als bedoeld in artikel 37 van de Algemene Verordening Gegevensbescherming.
- 1.4. *Meldplicht datalekken*: de meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens zoals bedoeld in artikelen 12, 33 en 34 van de Algemene Verordening Gegevensbescherming.
- 1.5. *Verwerkersovereenkomst*: een overeenkomst als bedoeld in artikel 28, derde lid, van de Algemene Verordening Gegevensbescherming.
- 1.6. *Bijlage(n)*: één of meer aanhangsel(s) bij deze Verwerkersovereenkomst die daar na parafering door Afnemer en Logius onderdeel van uitmaken.
- 1.7. *Verwerking*: elke handeling of elk geheel van handelingen met betrekking tot Persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen, of vernietigen van Persoonsgegevens.
- 1.8. *Betrokkene*: degene op wie een Persoonsgegeven betrekking heeft.
- 1.9. *Derde*: ieder, niet zijnde de Betrokkene, de Afnemer, Logius, of enig persoon die onder rechtstreeks gezag van de Afnemer of Logius gemachtigd is om Persoonsgegevens te verwerken.
- 1.10. *Ontvanger*: degene aan wie de Persoonsgegevens worden verstrekt.

Artikel 2. Reikwijdte en onderwerp van deze Verwerkersovereenkomst

- 2.1 De reikwijdte van deze Verwerkersovereenkomst is dat Logius optreedt als verwerker van Persoonsgegevens waarvoor Afnemer is aan te merken als verantwoordelijke in de zin van de Algemene Verordening Gegevensbescherming. In **Bijlage 1** bij deze Verwerkersovereenkomst staan het overzicht van de Dienst(en) die Logius levert aan Afnemer, de soorten te verwerken Persoonsgegevens, de categorieën van Betrokkenen, de subverwerkers en de aard en het doel van Verwerking van Persoonsgegevens beschreven.
- 2.2 Logius verplicht zich om bij het leveren van haar Dienst(en) aan de Afnemer de Persoonsgegevens te verwerken conform de redelijke schriftelijke instructies van

Afnemer die in overeenstemming zijn met de bepalingen van de Algemene Verordening Gegevensbescherming.

Artikel 3. Verplichtingen van Afnemer

- 3.1 Afnemer is in de zin van de Algemene Verordening Gegevensbescherming de verantwoordelijke voor de inhoud en gerelateerde Verwerking van Persoonsgegevens.
- 3.2 Afnemer houdt een register bij van de verwerkingsactiviteiten die onder haar verantwoordelijkheid plaatsvindt, zoals bepaald in artikel 30, eerste lid, Algemene Verordening Gegevensbescherming.
- 3.3 Afnemer garandeert dat de Persoonsgegevens rechtmatig zijn verkregen. Afnemer zal alle toepasselijke bepalingen betreffende de Verwerking van de Persoonsgegevens stipt in acht nemen. Afnemer zal Logius alle ter zake gevraagde informatie onverwijld schriftelijk of elektronisch verstrekken.
- 3.4 Afnemer zal Logius vrijwaren tegen iedere claim van een Derde (of een Betrokkene) die jegens Logius mocht worden ingesteld wegens schending van de Algemene Verordening Gegevensbescherming, door Afnemer die toerekenbaar is aan Afnemer.
- 3.5 Indien Afnemer voor de Verwerking van de Persoonsgegevens gebruik maakt van een intermediair of andere verwerker (niet zijnde Logius) die direct of indirect gebruik maakt van de Dienst:
 - a) blijft de verplichting in artikel 3.1 voor de Afnemer van kracht; en
 - b) sluit Afnemer een verwerkersovereenkomst met bovengenoemde intermediair of andere verwerker (niet zijnde Logius), waarbij deze genoemde intermediair of andere verwerker zich verplicht om de Algemene Verordening Gegevensbescherming na te leven. Afnemer zal ervoor zorg dragen dat deze intermediair of andere verwerker passende technische en organisatorische maatregelen - met inachtneming van relevante wet- en regelgeving en standaarden voor beveiliging - zal nemen om de Persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige Verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de Verwerking en de aard van de te beschermen gegevens met zich meebrengen. Deze maatregelen zijn er mede op gericht onnodige verzameling en verdere Verwerking van de Persoonsgegevens te voorkomen.

Artikel 4. Verplichtingen van Logius

- 4.1 Logius zal overeenkomstig het bepaalde in deze Verwerkersovereenkomst handelen bij de uitvoering van haar Dienst(en).
- 4.2 Logius stelt Afnemer, mits Afnemer het verzoek daartoe tijdig doet, te allen tijde in staat en assisteert bij het vervullen van haar plicht om aan verzoeken van de Betrokkene te voldoen, om binnen de wettelijke termijnen te voldoen aan de

verplichtingen op grond van de Algemene Verordening Gegevensbescherming, welke samenhangen met de Verwerking van Persoonsgegevens door Logius, meer in het bijzonder met betrekking tot de rechten van Betrokkenen, zoals, maar niet beperkt tot, een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens.

- 4.3 Logius verwerkt de Persoonsgegevens slechts in opdracht van Afnemer en zal alle redelijke instructies van Afnemer dienaangaande opvolgen, behoudens indien deze afwijken van wettelijke voorschriften.
- 4.4 Indien Logius de Dienst(en) geheel of ten dele heeft uitbesteed aan één of meer organisaties ("subverwerkers") die de Persoonsgegevens voor Logius verwerken, is Logius gehouden de verplichtingen van deze Verwerkersovereenkomst, voor zover relevant, aan bedoelde subverwerkers op te leggen, alsmede toe te zien op de naleving daarvan. Logius blijft te allen tijde aanspreekpunt en verantwoordelijk voor de naleving van de verplichtingen in deze Verwerkersovereenkomst welke aan haar zijn opgelegd. Indien een subverwerker niet is genoemd in **Bijlage 1** bij deze Verwerkersovereenkomst heeft Logius toestemming voor uitbesteding aan deze subverwerker nodig van de Afnemer die zijn toestemming niet op onredelijke gronden zal onthouden.
- 4.5 Op verzoek van Afnemer wordt binnen een daartoe door Afnemer bepaalde redelijke termijn door Logius (een deel van) de Persoonsgegevens aan een Derde overgedragen of worden deze Persoonsgegevens op een door Afnemer nader te bepalen wijze vernietigd.
- 4.6 Logius houdt een register bij van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van Afnemer heeft verricht, zoals bepaald in artikel 30, tweede lid, Algemene Verordening Gegevensbescherming.
- 4.7 Logius zal op verzoek van Afnemer alle in opdracht van Afnemer verwerkte Persoonsgegevens aan Afnemer ter beschikking stellen.
- 4.8 Indien Logius (pogingen tot) onrechtmatige of anderszins ongeautoriseerde Verwerkingen of inbreuken op de beveiligingsmaatregelen van de Persoonsgegevens signaleert, zal Logius Afnemer hierover inlichten en afhankelijk van de aard van de verwerking en de aan Logius ter beschikking staande informatie, Afnemer bijstand verlenen bij het voldoen aan de Meldplicht datalekken. Logius zal alle redelijkerwijs benodigde maatregelen treffen om (verdere) schending van de Algemene Verordening Gegevensbescherming, te voorkomen of te beperken.
- 4.9 Logius verwerkt geen Persoonsgegevens buiten een land van de Europese Unie/Europese Economische Ruimte, tenzij Logius daarvoor uitdrukkelijke schriftelijke toestemming heeft verkregen van Afnemer.

Artikel 5. Verstrekken van persoonsgegevens

- 5.1 Het is Logius niet toegestaan Persoonsgegevens te verstrekken aan Derden, tenzij in het kader van de Dienst overeengekomen of dit op schriftelijk of elektronisch verzoek van Afnemer wordt gedaan met inachtneming van de toepasselijke wetgeving of Afnemer schriftelijk of elektronisch toestemming tot de verstrekking door Logius heeft gegeven met inachtneming van de toepasselijke wetgeving. Logius is verplicht schriftelijk of elektronisch aan Afnemer te bevestigen dat een dergelijke verstrekking heeft plaatsgevonden aan Derden, waarbij de verstrekte Persoonsgegevens, de Betrokkene(n), de Ontvanger(s) en het moment van verstrekking worden beschreven.
- 5.2 Indien Logius op grond van een wettelijke verplichting Persoonsgegevens dient te verstrekken waarvoor Afnemer verantwoordelijke is, zal Afnemer in overleg met Logius de grondslag van het verzoek en de identiteit van de verzoeker verifiëren.

Artikel 6. Beveiliging

- 6.1 Logius legt op basis van een door haar uitgevoerde risicoanalyse - en met inachtneming van relevante wet- en regelgeving en standaarden voor beveiliging - passende technische en organisatorische maatregelen ten uitvoer om de Persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige Verwerking. Deze maatregelen, die zijn opgenomen in **Bijlage 2** bij deze Verwerkersovereenkomst, garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de Verwerking en de aard van de te beschermen gegevens met zich meebrengen. Deze maatregelen zijn er mede op gericht onnodige verzameling en verdere Verwerking van de Persoonsgegevens te voorkomen.
- 6.2 In aanvulling op het bepaalde in artikel 4.8, zijn de tussen Logius en Afnemer gemaakte afspraken ten behoeve van de uitvoering van de wettelijke Meldplicht datalekken opgenomen in **Bijlage 3** bij deze Verwerkersovereenkomst.

Artikel 7. Geheimhouding

- 7.1 Logius en een ieder die handelt onder haar gezag, voor zover deze toegang hebben tot Persoonsgegevens, voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de Persoonsgegevens waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit. Deze verplichting blijft na afloop of beëindiging van deze Verwerkersovereenkomst voortbestaan.
- 7.2 Indien Afnemer daarom schriftelijk of elektronisch verzoekt, zal Logius ten aanzien van de daarbij aangeduide Persoonsgegevens of informatie op kosten van Afnemer (extra) maatregelen treffen met het oog op de geheimhouding daarvan.

Artikel 8. Controle

- 8.1 Afnemer heeft het recht een controle op de nakoming van de verplichtingen van Logius onder deze Verwerkersovereenkomst uit te (laten) voeren door een onafhankelijke registeraccountant of (EDP-)auditor die is goedgekeurd door Logius. Logius is verplicht binnen een redelijke termijn aan deze controle alle medewerking te verlenen. Afnemer zal Logius een exemplaar van de resultaten van deze controle verstrekken. Indien Logius deze controle al zelf heeft laten verrichten door een onafhankelijke accountant of (EDP-)auditor, heeft Logius het recht om de bevindingen van deze accountant of (EDP-)auditor mede te delen aan Afnemer waarna voornoemd recht op controle komt te vervallen.
- 8.2 De kosten van een controle als bedoeld in artikel 8.1 komen voor rekening van Afnemer, tenzij blijkt dat Logius een belangrijk deel van haar verplichtingen op grond van deze Verwerkersovereenkomst niet nakomt en in strijd heeft gehandeld met de Algemene Verordening Gegevensbescherming. In dat geval komen de kosten voor rekening van Logius.

Artikel 9. Aansprakelijkheid

Indien Logius of Afnemer toerekenbaar tekortschiet in de nakoming van zijn verplichtingen onder deze Verwerkersovereenkomst of in strijd handelt met de Algemene Verordening Gegevensbescherming, geldt het bepaalde omtrent aansprakelijkheid zoals neergelegd in artikel 82 van de Algemene Verordening Gegevensbescherming.

Artikel 10. Rechten op gegevensdragers en Persoonsgegevens

- 10.1 Afnemer behoudt alle rechten van welke aard dan ook ten aanzien van de door hem onder deze Verwerkersovereenkomst aan Logius aangeleverde Persoonsgegevens.
- 10.2 In aanvulling op artikel 4.5 zal Logius bij beëindiging of ontbinding van deze Verwerkersovereenkomst op schriftelijk of elektronisch verzoek van Afnemer de Persoonsgegevens vernietigen.

Artikel 11. Duur en beëindiging van deze Verwerkersovereenkomst

- 11.1 Deze Verwerkersovereenkomst treedt in werking op de datum dat Afnemer en Logius de Verwerkersovereenkomst hebben ondertekend.
- 11.2 Deze Verwerkersovereenkomst blijft van kracht gedurende de periode dat Logius Dienst(en) levert aan Afnemer. Deze Verwerkersovereenkomst eindigt van rechtswege op het moment dat Logius geen Dienst(en) meer levert aan Afnemer, onverminderd het bepaalde in artikel 7.1.
- 11.3 Deze Verwerkersovereenkomst mag niet door Afnemer of Logius tussentijds worden opgezegd, onverminderd het recht van Afnemer en Logius om deze Verwerkersovereenkomst te ontbinden op grond van artikel 6:265 Burgerlijk Wetboek.

Artikel 12. Toepasselijk recht en jurisdictie

- 12.1 Op deze Verwerkersovereenkomst is Nederlands recht van toepassing.
- 12.2 Geschillen, die voortvloeien uit of samenhangen met deze Verwerkersovereenkomst, zullen bij uitsluiting worden voorgelegd aan de bevoegde rechter te Den Haag.

ALDUS OVEREENGEKOMEN DOOR PARTIJEN en opgemaakt in tweevoud,

Afnemer, te

.....,

Voor deze

Handtekening:

Naam:

Functie:

Datum:

Logius, te Den Haag:

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

namens deze, ir. Y.L. (Yvonne) van der Brugge-Wolring (Algemeen Directeur Logius),

namens deze,

Handtekening:

Naam: de heer G. Gihaux

Functie: Clustermanager Business/Relatie-Sourcing

Datum:

BIJLAGE 1 BIJ VERWERKERSOVEREENKOMST: DIENST EN VERWERKING VAN PERSOONSGEGEVENS

Naam van de Dienst(en): MijnOverheid

Datum: 03-01-2019

Versienummer: 1.3

Beschrijving van de Dienst(en) die Logius levert aan Afnemer:

Logius stelt Afnemer in staat om door middel van MijnOverheid (waaronder de Berichtenbox, Lopende Zaken en Persoonlijke Gegevens) elektronische diensten te leveren aan Gebruikers.

Berichten die zijn afgeleverd in een Berichtenbox worden niet overgedragen of ter beschikking gesteld aan Afnemer of Derden, maar worden alleen periodiek door Logius vernietigd na verloop van de toepasselijke wettelijke bewaartermijn.

Definities:

In deze **Bijlage 1** hebben onderstaande definities de onderstaande betekenissen:

MijnOverheid: de internetwebsite op het internetadres <https://mijn.overheid.nl> of www.mijnoverheid.nl waarmee Afnemer door middel van de Berichtenbox, Lopende Zaken en Persoonlijke Gegevens elektronische diensten levert aan Gebruikers.

Berichtenbox: de persoonlijke elektronische berichtenbox van een Gebruiker binnen MijnOverheid. In de Berichtenbox kan een Gebruiker elektronische berichten van Afnemer of andere afnemers ontvangen.

Lopende Zaken: de persoonlijke elektronische dienst binnen MijnOverheid waarmee een Gebruiker kan zien welke zaken of procedures hij bij Afnemer of andere afnemers heeft lopen.

Persoonlijke Gegevens: de persoonlijke elektronische dienst binnen MijnOverheid waarmee een Gebruiker kan zien welke persoonlijke gegevens van hem zijn geregistreerd bij Afnemer of andere afnemers.

Gebruiker: een natuurlijk persoon die is ingeschreven in de Basisregistratie Personen (BRP), uit dien hoofde beschikt over een burgerservicenummer (BSN) of een ander van overheidswege toegekend persoonsnummer en in het bezit is van een DigiD.

Soorten te verwerken Persoonsgegevens en categorieën van betrokkenen:

De volgende Persoonsgegevens worden verwerkt:

Burgerservicenummer	Staat mogelijk in de elektronische berichten die Afnemer plaatst in de Berichtenbox of in de informatie die in Lopende Zaken of Persoonlijke Gegevens van Gebruiker staan.
---------------------	--

Verwerkersovereenkomst

NAW-gegevens	Staan mogelijk in de elektronische berichten die Afnemer plaatst in de Berichtenbox of in de informatie die in Lopende Zaken of Persoonlijke Gegevens van Gebruiker staan.
Geboortedatum	Staat mogelijk in de elektronische berichten die Afnemer plaatst in de Berichtenbox of in de informatie die in Lopende Zaken of Persoonlijke Gegevens van Gebruiker staan.
Andere identificerende gegevens afhankelijk van de dienst die verzorgd wordt door Afnemer	Staan mogelijk in de elektronische berichten die Afnemer plaatst in de Berichtenbox of in de informatie die in Lopende Zaken of Persoonlijke Gegevens van Gebruiker staan.
Aanvullen indien nodig	

Aard en het doel van Verwerking van Persoonsgegevens:

Het doel van de Verwerking van Persoonsgegevens is:

- het juist en conform overeengekomen afspraken afleveren van berichten van de Afnemer in de Berichtenbox en/of Lopende Zaken;
- het tonen van Persoonsgegevens in Persoonlijke Gegevens;
- de goede werking van een (toekomstige) functionaliteit binnen MijnOverheid ten behoeve van de Gebruiker mits deze nieuwe functionaliteit verenigbaar is met de wet.

Organisaties ("subverwerkers") die de Persoonsgegevens voor Logius verwerken:

Logius maakt gebruik van de volgende subverwerkers:

- de combinatie Equinix Netherlands B.V. en European Business Process Institute (EBPI) B.V., gevestigd te Enschede en Den Haag (ICT dienstverlener).
- European Business Process Institute (EBPI) B.V., gevestigd te Den Haag (ICT dienstverlener).

Met alle hierboven genoemde subverwerkers zijn verwerkersovereenkomsten afgesloten.

BIJLAGE 2 BIJ VERWERKERSOVEREENKOMST: INFORMATIEBEVEILIGING

Maatregelen en risico-analyse:

De technische en organisatorische maatregelen om de Persoonsgegevens (zoals bedoeld in de Verwerkersovereenkomst) te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking zijn opgenomen in de Baseline Informatiebeveiliging Rijksdienst (hierna: BIR2017). Logius dient als onderdeel van de Rijksoverheid te voldoen aan de BIR2017. BIR2017 wordt mettertijd vervangen door de Baseline Informatiebeveiliging Overheid (BIO), die de sectorale baselines BIR, BIG, BIWA en IBI vervangt.

De BIR2017 biedt één normenkader voor de beveiliging van de informatiehuishouding van de Rijksoverheid. Dit maakt het mogelijk om veilig samen te werken en onderling gegevens uit te wisselen. De BIR2017 zorgt voor één heldere set afspraken zodat een bedrijfsonderdeel weet dat de gegevens die verstuurd worden naar een ander onderdeel van de Rijksoverheid op het juiste beveiligingsniveau (vertrouwelijkheid, integriteit en beschikbaarheid) worden behandeld.

MijnOverheid verwerkt persoonsgegevens. Als algemeen kader geldt daarvoor de Algemene Verordening Gegevensbescherming (inclusief de artikelen 12, 33 en 34 inzake Meldplicht datalekken). Voor bijzondere berichten of gegevens kan nog bijzondere regelgeving van toepassing zijn (politierregisters, BRP, e.a.). In de overgrote meerderheid van de gevallen zijn de afnemers van MijnOverheid voor het tonen, sturen en verwerken van persoonsgegevens aan dit zelfde kader onderworpen - en volledig zelf verantwoordelijk. De informatiebeveiliging van de Afnemer blijft daarmee de verantwoordelijkheid van de Afnemer zelf. Om een veilige aansluiting op het door Logius gehanteerde BIR-normenkader te bewerkstelligen adviseert Logius de informatiebeveiliging aan Afnemerzijde in te richten conform de van toepassing zijnde normenkaders als BIR, BIG, BIWA, ISO27001 of anderszins.

In de Wet elektronisch berichtenverkeer belastingdienst is de rol van de minister van Binnenlandse Zaken en Koninkrijksrelaties voor de veilige werking van MijnOverheid met zoveel woorden bepaald. Deze rol is op hoofdlijnen uitgewerkt in Hoofdstuk 5 (Werking, beveiliging en betrouwbaarheid) van de Regeling voorzieningen GDI (zie Staatscourant Nr. 37158 van 29 oktober 2015).

Voor de hierboven genoemde algemene kaders van informatiebeveiliging voor afnemers van MijnOverheid kan onder meer verwezen worden naar veel gebruikte open standaarden als DNSSEC, TLS, SAML, SPF en DKIM, naar de NEN-ISO/IEC 27002.

Voor de Rijksoverheid (organen en instellingen) is de BIR, met VIR en VIRBI het geldende oriëntatiekader. Logius verleent assistentie aan de Afnemer bij het uitvoeren van een risico-analyse.

Voor gemeenten is relevant de Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten (vgl. Gemma referentie componenten beveiliging).

Voor Provincies en Waterschappen zijn relevant de Interprovinciale Baseline Informatiebeveiliging en de Baseline Informatiebeveiliging Waterschappen.

Voor Pensioenfondsen conform de Wet Financieel Toezicht en de Pensioenwet is DNB van oordeel dat de financiële instellingen dienen te beschikken over adequate procedures en maatregelen ter beheersing van de IT-risico's conform Toetsingskader Informatiebeveiliging 2014 van DNB. Een voorbeeld van dergelijke standaarden zijn Cobit en ISO27000.

BIJLAGE 3 BIJ VERWERKERSOVEREENKOMST: UITVOERING VAN DE MELDPlicht DATALEKKEN

Artikel 1. Op de hoogte stellen van de Afnemer ingeval van een datalek

Logius beoordeelt bij een beveiligingsincident met in achtneming van de artikelen 12, 33 en 34 van de Algemene Verordening Gegevensbescherming en de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 (hierna: Richtsnoeren) of een onbevoegde toegang tot of onbedoelde vernietiging, wijziging of vrijkomen van persoonsgegevens een datalek is in de zin van vornoemde artikelen 12, 33 en 34 Algemene Verordening Gegevensbescherming en de Richtsnoeren en wie de verwerkingsverantwoordelijke is.

Logius zal Afnemer direct over dit datalek inlichten en, afhankelijk van de aard van de verwerking en de aan Logius ter beschikking staande informatie, Afnemer bijstand verlenen bij het voldoen aan de Meldplicht datalekken. Logius zal alle redelijkerwijs benodigde maatregelen treffen om (verdere) schending van de Algemene Verordening Gegevensbescherming te voorkomen of te beperken.

Artikel 2. Melding doen aan Autoriteit Persoonsgegevens en aan betrokkenen

De Afnemer besluit in overleg met Logius wie van beiden de melding van het datalek doet aan de Autoriteit Persoonsgegevens en, indien nodig, aan de betrokkenen.

Artikel 3. Gegevens overleggen aan de Afnemer

Logius overlegt in de situaties, beschreven in artikel 1 hierboven, zo spoedig mogelijk aan de Afnemer haar bevindingen inzake het datalek tezamen met de reeds door Logius getroffen maatregelen met in achtneming van de Richtsnoeren van de Autoriteit Persoonsgegevens.

Artikel 4. Informeren van de Afnemer over nieuwe maatregelen

Logius stelt, in aanvulling op het bepaalde in artikel 3 hierboven, Opdrachtgever zo spoedig mogelijk en regelmatig op de hoogte van de actuele stand van zaken met betrekking tot het geconstateerde datalek en de eventuele nieuwe door Logius te treffen maatregelen met betrekking tot het geconstateerde datalek.