Verwerkersovereenkomst
Omgevingsdienst regio Utrecht

Omgevingsdienst regio Utrecht
januari 2020

Verwerkersovereenkomst

Partijen:

I. **Omgevingsdienst regio Utrecht (ODRU)**, statutair gevestigd te Utrecht en kantoorhoudende aan de Archimedeslaan 6 te (3584 BA) Utrecht, geregistreerd bij de Kamer van Koophandel onder nr. 55523544, hierbij rechtsgeldig vertegenwoordigd door diens directeur dhr. A. van Vuuren, hierna te noemen “Verwerkingsverantwoordelijke”;

en

II. ******* statutair gevestigd te *** en kantoorhoudende aan Heidebloem 15 te (5482 ZA) Schijndel, geregistreerd bij de Kamer van Koophandel onder nr. 16068733 hierbij rechtsgeldig vertegenwoordigd door *** hierna te noemen “Verwerker”;

in aanmerking nemende dat

- Verwerkingsverantwoordelijke Persoonsgegevens door Verwerker wil laten verwerken, ten behoeve van de uitvoering van de overeenkomst “***” die met Verwerker is gesloten en getekend op ***, alsmede de hiermee verbonden c.q. de daaruit vloeiende deelovereenkomsten (hierna: “de Overeenkomst’’).
- Verwerker die in het kader van de uitvoering van de Overeenkomst met Verwerkingsverantwoordelijke Persoonsgegevens verwerkt, is aan te merken als Verwerker in de zin van de Algemene Verordening Gegevensbescherming (AVG) en Omgevingsdienst regio Utrecht (ODRU) als Verwerkingsverantwoordelijke in de zin van de AVG.
- Verwerker en Verwerkingsverantwoordelijke (hierna: “Partijen”), mede gelet op het vereiste uit artikel 28 lid 3 van de AVG, hun rechten en plichten schriftelijk wensen vast te leggen middels deze Verwerkersovereenkomst (hierna: “Verwerkersovereenkomst”).
- De algemene bepalingen uit de Verwerkersovereenkomst gelden voor alle Verwerkingen in de uitvoering van de Overeenkomst.

Verklaren te zijn overeengekomen een Verwerkersovereenkomst als bedoeld in artikel 28 aanhef van lid 3 van de AVG en komen in die zin het volgende overeen:

Artikel 1. Definities

De hierna en hiervoor in deze Verwerkersovereenkomst vermelde, met een hoofdletter geschreven begrippen, hebben de volgende betekenis:

1.1 AVG: 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). Elke verwijzing naar de AVG is van kracht per 25 mei 2018.

1.2 Bestand: elk gestructureerd geheel van Persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.

1.3 Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.

1.4 Bijlagen: aanhangsels bij deze Verwerkersovereenkomst, die na door beide Partijen te zijn geparafeerd, deel uitmaken van deze Verwerkersovereenkomst.

1.5 Bijzondere Persoonsgegevens: Persoonsgegevens zoals bedoeld in artikel 9 lid 1 van de AVG.
1.6 Datalek: een inbreuk op de beveiliging, bedoeld in artikel 4 lid 12 jo. artikel 33 lid 1 van de AVG.
1.7 Derde: ieder, niet zijnde de Betrokkene, de Verwerkingsverantwoordelijke, de Verwerker, of enig persoon die onder rechtstreeks gezag van de Verwerkingsverantwoordelijke of de Verwerker gemachtigd is om Persoonsgegevens te verwerken.
1.8 Dienst: is de onder de Overeenkomst te leveren dienst door de Verwerker.
1.9 Europese Economische Ruimte (EER): alle landen van de Europese Unie, Liechtenstein, Noorwegen en IJsland.
1.10 Gebruiker: is een op enigerlei wijze aan Verwerkingsverantwoordelijke verbonden (natuurlijke) persoon, zoals personeel, die door de Verwerkingsverantwoordelijke geautoriseerd is tot (een bepaald deel van) de Dienst.
1.11 Onderaannemer: een partij die door Verwerker is ingeschakeld om te ondersteunen bij het uitvoeren van de Dienst. Indien de Onderaannemer in opdracht van Verwerker Persoonsgegevens verwerkt, is de Onderaannemer tevens aan te merken als Derde.
1.12 Overeenkomst: de raamovereenkomst en deelovereenkomst(en) waarvan deze Verwerkersovereenkomst onderdeel uitmaakt.
1.13 Partijen of Partij: Verwerkingsverantwoordelijke en/of de Verwerker.
1.14 Persoonsgegevens: Persoonsgegevens in de zin van de AVG.
1.15 Verwerker: degene die ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen in de zin van artikel 4 lid 8 van de AVG.
1.16 Verwerkersovereenkomst: de onderhavige overeenkomst.
1.17 Verwerking van Persoonsgegevens of het verwerken van Persoonsgegevens of Verwerking: elke handeling of elk geheel van handelingen met betrekking tot een bewerking of een geheel van bewerkingen met betrekking tot Persoonsgegevens in de zin van artikel 4 lid 2 van de AVG.
1.18 Verwerkingsverantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander in de zin van artikel 4 lid 7 van de AVG.
1.19 Verstrekken van Persoonsgegevens: het bekend maken of ter beschikking stellen van Persoonsgegevens.
1.20 Toezichthoudende autoriteit: een onafhankelijke overheidsinstantie verantwoordelijk voor het toezicht op de naleving van de wet in verband met de verwerking van Persoonsgegevens. In Nederland is dit de Autoriteit Persoonsgegevens.

Artikel 2. Algemeen

2.1 Verwerker verwerkt in het kader van de uitvoering van de Dienst Persoonsgegevens in opdracht van de Verwerkingsverantwoordelijke in overeenstemming met diens nadere schriftelijke instructies, behoudens afwijkende wettelijke verplichtingen conform artikel 28 lid 3 sub a van de AVG.
2.2 De Verwerker heeft geen zeggenschap over de ter beschikking gestelde Persoonsgegevens. Zo neemt hij geen beslissingen over ontvangst en gebruik van de gegevens, de Verstrekking van Persoonsgegevens aan Derden en de duur van de opslag van gegevens, tenzij wettelijke bepalingen iets anders voorschrijven. De zeggenschap over de Persoonsgegevens verstrekt onder de Overeenkomst komt nimmer bij de Verwerker te berusten.
2.3 Verwerker verbindt zich om in het kader van de uitvoering van de Overeenkomst de door de Verwerkingsverantwoordelijke ter beschikking gestelde Persoonsgegevens behoorlijk en zorgvuldig en in overeenstemming met de AVG en andere toepasselijke regelgeving betreffende de Verwerking van Persoonsgegevens te verwerken.

2.4 De Verwerking heeft tot doel de Dienst zoals omschreven in de Overeenkomst aan de Verwerkingsverantwoordelijke te verlenen. Verwerking door Verwerker zal daarom uitsluitend plaatsvinden voor zover noodzakelijk om deze Dienst te kunnen leveren. Voor de uitvoering van de Dienst kunnen uitsluitend de categorieën Persoonsgegevens worden Verwerkt die in Bijlage A zijn gespecificeerd.

2.5 Verwerker zal Persoonsgegevens die hem in het kader van de Overeenkomst ter beschikking zijn gesteld niet langer bewaren dan noodzakelijk is

(i) voor de uitvoering van de Overeenkomst; of

(ii) om een op hem rustende wettelijke verplichting na te komen.

De bewaartermijnen van de gegevensverwerking staan gespecificeerd in bijlage A.

2.6 Verwerker zal de Persoonsgegevens uitsluitend verwerken in opdracht en volgens de instructies van Verwerkingsverantwoordelijke. Verwerker mag de Persoonsgegevens niet ten eigen nutte, ten nutte van Derden, en/of voor eigen dan wel reclamedoeleinden c.q. andere doeleinden verwerken, behoudens op hem rustende afwijkende dwingendrechtelijke verplichtingen. De doeleinden van de gegevensverwerking staan gespecificeerd in bijlage A.

2.7 Verwerker is verplicht Verwerkingsverantwoordelijke onmiddellijk te informeren over toekomstige wijzigingen in de uitvoering van de Overeenkomst, zodat Verwerkingsverantwoordelijke kan toezien op de naleving van afspraken met Verwerker. Hieronder wordt mede begrepen de inschakeling van (nieuwe) Onderaannemers, onverminderd het bepaalde in artikel 7 (Inschakeling Onderaannemers) en artikel 12 (Wijziging overeenkomst).

2.8 De Verwerker zal te allen tijde op eerste verzoek van de Verwerkingsverantwoordelijke onmiddellijk alle van de Verwerkingsverantwoordelijke afkomstige Persoonsgegevens met betrekking tot deze Verwerkersovereenkomst ter hand stellen.

2.9 De Verwerker stelt de Verwerkingsverantwoordelijke te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG, meer in het bijzonder ten aanzien van de rechten van Betrokkenen, zoals, maar niet beperkt tot een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens.

2.10 De Verwerker is conform artikel 30 lid 2 van de AVG gehouden om een register van alle categorieën van verwerkingsactiviteiten die hij ten behoeve van de Verwerkingsverantwoordelijke heeft verricht bij te houden. Dit register bevat de in artikel 30 lid 2 van de AVG opgenomen gegevens.

2.11 Rekening houdend met de aard van de verwerking en de ter beschikking staande informatie, verstrekt de Verwerker de Verwerkingsverantwoordelijke de benodigde informatie in het kader van het kunnen uitvoeren van een Privacy Impact Assessment door de Verwerkingsverantwoordelijke.

Artikel 3. Ingangsdatum, duur en beëindiging

3.1 Deze Verwerkersovereenkomst treedt in werking op de datum waarop Partijen deze ondertekenen. De duur van de Verwerkersovereenkomst is gelijk aan de duur van de Overeenkomst en duurt voort zolang Verwerker als verwerker van Persoonsgegevens optreedt in het kader van de door Verwerkingsverantwoordelijke ter beschikking gestelde Persoonsgegevens in verband met het uitvoeren van de Dienst. De Verwerkersovereenkomst is niet los van de Overeenkomst te beëindigen.

3.2 Na beëindiging van deze Verwerkersovereenkomst zullen de lopende verplichtingen voor Verwerker, zoals het melden van Datalekken waarbij Persoonsgegevens van Verwerkingsverantwoordelijke betrokken zijn en de plicht tot geheimhouding, blijven voortduren.

3.3 Bij beëindiging van de Overeenkomst om welke reden ook, dan wel op eerste verzoek van Verwerkingsverantwoordelijke gedurende de looptijd van de Overeenkomst, zal Verwerker -

tegen een beperkte vergoeding die de door Verwerker hiervoor redelijkerwijs en aantoonbaar gemaakte kosten niet overschrijden - ervoor zorgdragen dat naar keuze van Verwerkingsverantwoordelijke op voor Verwerkingsverantwoordelijke eenvoudige bruikbare wijze

(i) alle of een door Verwerkingsverantwoordelijke bepaald gedeelte hem in het kader van de Dienst ter beschikking gestelde (Persoons)gegevens worden vernietigd op alle locaties (inclusief eventuele back-ups),

(ii) alle of een door Verwerkingsverantwoordelijke bepaald gedeelte van hem in het kader van de Dienst ter beschikking gestelde (Persoons)gegevens aan een opvolgend dienstverlener ter beschikking worden gesteld, dan wel

(iii) Verwerkingsverantwoordelijke en/of Gebruikers in de gelegenheid worden gesteld om hun (Persoons)gegevens of een door Verwerkingsverantwoordelijke bepaald gedeelte van de (Persoons)gegevens aan de Dienst te onttrekken, één en ander tenzij opslag van de Persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht (artikel 28 lid 3 sub g van de AVG). De Verwerker zal de (Persoons)gegevens gestructureerd beschikbaar stellen in een open standaardformaat (dataportabiliteit). Een eventuele discussie omtrent de hoogte van de vergoeding als in dit artikellid bedoeld, is geen reden om vernietiging en/of het beschikbaar stellen van de in dit artikellid opgenomen data te weigeren.

3.4 Verwerker zal de in het vorige lid beschreven dataportabiliteit waarborgen zodanig dat er geen sprake is van verlies van functionaliteit of (delen van) de (Persoons)gegevens.

3.5 Verwerker zal na de teruggave en/of vernietiging van de Persoonsgegevens schriftelijk aan Verwerkingsverantwoordelijke verklaren niet langer in het bezit te zijn van de Persoonsgegevens.

Artikel 4. Geheimhoudingsplicht

4.1 Personen in dienst van, dan wel werkzaam ten behoeve van de Verwerker, evenals de Verwerker zelf, zullen alle gegevens die hen in het kader van de uitvoering van de Overeenkomst of Verwerkersovereenkomst ter kennis of beschikking komen, geheimhouden en op geen enkele wijze verder intern of extern bekendmaken en/of aan derden verstrekken, behalve voor zover:

a) Bekendmaking en/of verstrekking van die gegevens in het kader van de uitvoering van de Overeenkomst noodzakelijk is;

b) Enig dwingendrechtelijk Nederlands wettelijk voorschrift of Nederlandse rechterlijke uitspraak Partijen tot bekendmaking en/of verstrekking van die gegevens of informatie verplicht, waarbij Partijen eerst de andere partij hiervan op de hoogte stellen;

c) Bekendmaking en/of verstrekking van die gegevens geschiedt met voorafgaande schriftelijke toestemming van de andere Partij; dan wel

d) Het informatie betreft die al rechtmatig openbaar was op een andere wijze dan door het handelen of nalaten van een der Partijen.

4.2 Indien de Verwerker op grond van een wettelijke verplichting gegevens dient te Verstrekken, zal de Verwerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal de Verwerker de Verwerkingsverantwoordelijke onmiddellijk, voorafgaand aan de Verstrekking, ter zake informeren, tenzij wettelijke bepalingen dit verbieden.

4.3 Als Verwerker zijn geheimhoudingsverplichting schendt, is hij een direct opeisbare boete van € 25.000 (zegge: vijfentwintigduizend Euro) per overtreding aan de andere Partij verschuldigd. In afwijking van artikel 6:92 BW komen Partijen overeen dat het een Partij vrij staat om naast boetes, volledige schadevergoeding te vorderen en wordt het recht op nakoming of (gedeeltelijke) ontbinding onverlet gelaten.

4.4 Verwerker zal de voor hem werkzame personen (waaronder werknemers) die betrokken zijn bij de Verwerking van vertrouwelijke gegevens (inclusief Persoonsgegevens) contractueel verplichten tot geheimhouding van die vertrouwelijke gegevens.

4.5 Verwerker verleent op verzoek van Verwerkingsverantwoordelijke zijn medewerking aan het uitoefenen van toezicht door een onafhankelijke derde op de bewaring en het gebruik van vertrouwelijke gegevens door de Verwerker.

4.6 De Verwerker stelt alle gegevens die hij in het kader van de uitvoering van de Overeenkomst onder zich heeft, inclusief eventueel daarvan gemaakte kopieën, op eerste verzoek aan de Verwerkingsverantwoordelijke ter beschikking.

Artikel 5. Beveiligingsmaatregelen

5.1 De Verwerker legt passende technische en organisatorische maatregelen ten uitvoer om Persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige Verwerking, conform artikel 28 lid 3 sub c jo. artikel 32 van de AVG. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging daarvan, een passend beveiligingsniveau gelet op de risico's die de Verwerking en de aard van de te beschermen Persoonsgegevens meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere Verwerking te voorkomen. Verwerker legt de maatregelen schriftelijk vast en draagt er zorg voor dat de beveiliging zoals bedoeld in dit artikellid voldoet aan de beveiligingseisen op grond van artikel 32 van de AVG. In Bijlagen A en C zijn de beveiligingsmaatregelen beschreven die de Verwerker moet toepassen.

5.2 Verwerker zal Verwerkingsverantwoordelijke desgevraagd onverwijld schriftelijk informatie verstrekken met betrekking tot (de organisatie van) de beveiliging van Persoonsgegevens.

5.3 Op eerste verzoek van Verwerkingsverantwoordelijke zal de Verwerker jaarlijks over de opzet en werking van het stelsel van maatregelen en procedures, gericht op naleving van deze Verwerkersovereenkomst, rapporteren (bijvoorbeeld in de vorm van een ISAE 3402 Type II assurance report van een onafhankelijke IT-auditor). Hiervoor brengt Verwerker geen kosten in rekening aan Verwerkingsverantwoordelijke.

5.4 Indien blijkt dat een wijziging in de te nemen beveiligingsmaatregelen noodzakelijk is, omdat het beveiligingsniveau niet toereikend is, treden Partijen in overleg over de wijziging daarvan. De kosten gemoeid met het wijzigen van de beveiligingsmaatregelen komen voor rekening van de Partij waarbij de oorzaak van het ontoereikende beveiligingsniveau ligt.

Artikel 6. Meldplicht Datalekken

6.1 In het geval van een vermoedelijk(e) of daadwerkelijk(e)

(i) Datalek
(ii) schending van de beveiligingsmaatregelen
(iii) schending van de geheimhoudingsplicht of
(iv) verlies van vertrouwelijke gegevens

zal Verwerker de Verwerkingsverantwoordelijke direct, doch uiterlijk binnen 24 uur na de eerste ontdekking van het incident, informeren. Melding geschiedt overeenkomstig het proces beschreven in Bijlage A. De Verwerker zal op eigen kosten alle redelijkerwijs benodigde maatregelen treffen om (verdere) onbevoegde kennisneming, wijziging, en verstrekking van Persoonsgegevens dan wel anderszins onrechtmatige Verwerking te voorkomen of te beperken en een schending van beveiligingsmaatregelen, schending van de geheimhoudingsplicht of verder verlies van vertrouwelijke gegevens te beëindigen en in de toekomst te voorkomen, onverminderd enig recht van Verwerkingsverantwoordelijke op

schadevergoeding of andere maatregelen. Deze bepaling is van toepassing op incidenten bij de Verwerker en zijn eventuele Onderaannemers (Derden).

6.2 De door Verwerker te verstrekken informatie inzake het onder 6.1 genoemde informatie behelst in ieder geval de in de Bijlage B beschreven gegevens voor zover toepasselijk. Verwerker spant zich in de informatie zo volledig, correct en accuraat als redelijkerwijs mogelijk te verstrekken. Verwerker zal Verwerkingsverantwoordelijke op de hoogte houden van nieuwe ontwikkelingen rondom het Datalek, ook zal Verwerker de getroffen maatregelen om het Datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen, overleggen aan Verwerkingsverantwoordelijke.

6.3 Verwerker zal op verzoek van Verwerkingsverantwoordelijke meewerken aan het informeren van de bevoegde autoriteiten en Betrokkene(n). Verwerker mag zelf geen melding van een Datalek aan de Toezichthouder doen, wanneer bij het Datalek Persoonsgegevens van Verwerkingsverantwoordelijke betrokken zijn. Ook mag Verwerker de Betrokkenen niet informeren over het Datalek. Deze verantwoordelijkheid ligt bij Verwerkingsverantwoordelijke.

6.4 Verwerker maakt schriftelijke afspraken met Onderaannemers over het melden van incidenten aan Verwerker, die de Verwerker en de Verwerkingsverantwoordelijke in staat stellen verplichtingen in het geval van een incident zoals beschreven in lid 1 na te leven.

6.5 Conform artikel 28 lid 3 sub f van de AVG, verleent de Verwerker, rekening houdend met de aard van de Verwerking en de hem ter beschikking staande informatie, de Verwerkingsverantwoordelijke bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de AVG.

Artikel 7. Inschakeling Onderaannemers

7.1 De Verwerker is slechts gerechtigd de uitvoering van de werkzaamheden geheel of ten dele uit te besteden aan een Onderaannemer na voorafgaande schriftelijke specifieke of algemene toestemming van de Verwerkingsverantwoordelijke. In geval van algemene schriftelijke toestemming licht de Verwerker de Verwerkingsverantwoordelijke in over beoogde veranderingen inzake de toevoeging of vervanging van Onderaannemers, waarbij de Verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken.

7.2 Verwerkingsverantwoordelijke verleent hierbij algemene toestemming voor het inschakelen van leveranciers als Onderaannemer, welke zijn opgenomen in Bijlage A.

7.3 Zonder de voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke verleent Verwerker aan Derden, waaronder Onderaannemers en aan groepsmaatschappijen waartoe Verwerker behoort, zoals dochter- of zustermaatschappijen, geen toegang tot de Persoonsgegevens. Verwerkingsverantwoordelijke zal deze toestemming niet op onredelijke gronden onthouden. Bij het verlenen van toestemming is Verwerkingsverantwoordelijke gerechtigd hieraan voorwaarden te verbinden of de toestemming in tijd te beperken.

7.4 De Verwerker blijft in deze gevallen te allen tijde aanspreekpunt en verantwoordelijk voor de naleving van de bepalingen uit deze Verwerkersovereenkomst. Verwerker zal Verwerkingsverantwoordelijke informeren, zodra niet langer van de diensten van een Onderaannemer gebruikt wordt gemaakt.

7.5 Voor de inschakeling van Onderaannemers bij het leveren van de Dienst gelden de volgende voorwaarden:

- Verwerker sluit een Verwerkersovereenkomst met zijn Onderaannemers die voldoet aan de vereisten van artikel 28 van de AVG.
- Verwerker geeft pas toegang aan de Onderaannemer na de toestemming van Verwerkingsverantwoordelijke; en
- Verwerkingsverantwoordelijke heeft de mogelijkheid om gemaakte afspraken tussen Verwerker en de Onderaannemer op te vragen.

7.6 De door Verwerkingsverantwoordelijke gegeven toestemming laat onverlet de verantwoordelijkheid en aansprakelijkheid van Verwerker voor de nakoming van de Verwerkersovereenkomst.

7.7 Verwerker vrijwaart Verwerkingsverantwoordelijke voor alle aanspraken van Derden, daaronder begrepen Betrokkenen, die jegens Verwerkingsverantwoordelijke mochten worden ingesteld wegens een aan Verwerker of door hem ingeschakelde Onderaannemer, toe te rekenen schending van de AVG of andere toepasselijke regelgeving betreffende de Verwerking van Persoonsgegevens.

Artikel 8. Audit

8.1 De Verwerkingsverantwoordelijke is te allen tijde gerechtigd de Verwerking van Persoonsgegevens te (doen) controleren. De Verwerker is verplicht de Verwerkingsverantwoordelijke, de Autoriteit Persoonsgegevens, of de door Verwerkingsverantwoordelijke ingeschakelde derde (onder geheimhouding) toe te laten en verplicht medewerking te verlenen zodat de controle daadwerkelijk uitgevoerd kan worden.

8.2 De Verwerkingsverantwoordelijke zal een dergelijke controle slechts (laten) uitvoeren na een voorafgaande schriftelijke melding aan de Verwerker. Een controle zal niet onredelijk vaak plaatsvinden en zal slechts op korte termijn worden aangekondigd wanneer hiervoor dwingende redenen bestaan.

8.3 De Verwerker verbindt zich om binnen een door de Verwerkingsverantwoordelijke te bepalen termijn de Verwerkingsverantwoordelijke, of de door de Verwerkingsverantwoordelijke ingeschakelde derde, te voorzien van de verlangde informatie conform artikel 28 lid 3 sub h van de AVG, zulks met uitzondering van inzage in dan wel afgifte van (delen van) de broncode. Hierdoor kan de Verwerkingsverantwoordelijke, of de door de Verwerkingsverantwoordelijke ingeschakelde derde, zich een oordeel vormen over de naleving door de Verwerker zoals omschreven in de Overeenkomst en Verwerkersovereenkomst. De Verwerker stelt de Verwerkingsverantwoordelijke onmiddellijk in kennis indien naar zijn mening een instructie inbreuk oplevert op de AVG of op andere Unierechtelijke of lidstaatrechtelijke bepalingen inzake gegevensbescherming (artikel 28 lid 3 sub h en de laatste alinea van lid 3 van de AVG). De Verwerkingsverantwoordelijke, of de door de Verwerkingsverantwoordelijke ingeschakelde derde, is gehouden alle informatie betreffende deze controles vertrouwelijk te behandelen.

8.4 Verwerker staat er voor in, de door de Verwerkingsverantwoordelijke of ingeschakelde derde, aangegeven aanbevelingen te verbetering binnen de daartoe door de Verwerkingsverantwoordelijke te bepalen redelijke termijn uit te voeren.

8.5 De Verwerker rapporteert jaarlijks over de opzet en werking van het stelsel van maatregelen en procedures, gericht op de naleving van de Overeenkomst en Verwerkersovereenkomst. Deze rapportage dient te worden ondertekend door een directielid binnen de organisatie van Verwerker. De jaarlijkse rapportage is niet van toepassing indien Verwerker in het bezit is van een geldig ISO 27001 certificaat. De Verwerker heeft nog wel de verplichting om te voldoen aan artikel 8.6 van onderliggende Verwerkersovereenkomst.

8.6 Naast rapportages van de Verwerker en controles door de Verwerkingsverantwoordelijke of de door de Verwerkingsverantwoordelijke ingeschakelde derde, kunnen beide Partijen ook overeenkomen gebruik te maken van een Third Party Memorandum (TPM) , jaarlijks opgesteld door een onafhankelijke externe deskundige. Dit sluit de mogelijkheid tot controle zoals beschreven in artikel 8.1 niet uit wanneer hier een dwingende reden voor bestaat.

8.7 De kosten van de rapportage (zie artikel 8.5) of TPM audits (zie artikel 8.6), komen voor rekening van de Verwerker. De kosten van (additionele) controles op initiatief van Verwerkingsverantwoordelijke (zie de mogelijkheid beschreven in de laatste zin van artikel 8.6), komen voor rekening van de Verwerkingsverantwoordelijke, tenzij uit de bevindingen van de audit blijkt dat de Verwerker de bepalingen uit de Verwerkersovereenkomst niet is nagekomen. In dat geval komen de kosten voor rekening van Verwerker. Deze bepaling laat

de overige rechten van de Verwerkingsverantwoordelijke, waaronder die op schadevergoeding, onverlet.

Artikel 9. Internationaal verkeer

9.1 Verwerker garandeert dat iedere Verwerking van Persoonsgegevens welke door of namens Verwerker met inbegrip van de door hem ingeschakelde Onderaannemers wordt verricht in verband met het uitvoeren van de Overeenkomst binnen de Europese Economische Ruimte (EER) plaats zal vinden. Het is derhalve niet toegestaan om Persoonsgegevens door te geven naar of op te slaan in een land buiten de EER of Persoonsgegevens toegankelijk maken vanuit een niet-EER land. Verwerker verschaft voorafgaand aan het sluiten van de Verwerkersovereenkomst inzicht in de locatie(s) waar de verwerking plaatsvindt (te vermelden in Bijlage A).

9.2 De transmissie van gegevens zal uitsluitend versleuteld plaatsvinden waarbij voor de versleuteling geavanceerde (zijnde minstens zo geavanceerd als in de markt gebruikelijk) technieken zullen worden gebruikt.

Artikel 10. Opsporingsverzoeken

10.1 Indien Verwerker een verzoek of een bevel van een Nederlandse of buitenlandse toezichthouder, overheidsinstantie of een opsporings-, strafvorderings- of nationale veiligheidsinstantie ontvangt om (inzage in) Persoonsgegevens te verschaffen, dan zal Verwerker de Verwerkingsverantwoordelijke onverwijld informeren. Bij de behandeling van het verzoek of bevel zal Verwerker alle instructies van Verwerkingsverantwoordelijke in acht nemen (waaronder de instructie om de behandeling van het verzoek of bevel geheel of gedeeltelijk aan Verwerkingsverantwoordelijke over te laten) en alle redelijkerwijs benodigde medewerking verlenen.

10.2 Indien het Verwerker op grond van het verzoek of bevel is verboden om te voldoen aan zijn verplichtingen op grond van het bovenstaande, dan zal Verwerker de redelijke belangen van Verwerkingsverantwoordelijke behartigen. Verwerker zal daartoe in ieder geval:

a) Juridisch laten 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 het bovenstaande te voldoen;
b) Alleen aan het verzoek of bevel meewerken indien hij hiertoe wettelijk verplicht is en waar mogelijk (in rechte) bezwaar maken tegen het verzoek of bevel of het verbod om Verwerkingsverantwoordelijke hierover te informeren of zijn instructies op te volgen;
c) Niet meer of andere Persoonsgegevens Verstrekken dan strikt noodzakelijk om aan het verzoek of bevel te voldoen;
d) Indien sprake is van doorgifte naar een land buiten de EER: de mogelijkheden onderzoeken om te voldoen aan hoofdstuk 5 (artikel 44 e.v.) van de AVG;
e) Verwerkingsverantwoordelijke onverwijld informeren zodra dit is toegestaan.

10.3 In dit artikel wordt onder “wettelijk” niet alleen Nederlandse, maar ook buitenlandse wet- en regelgeving verstaan. In afwijking van hetgeen elders is opgenomen in deze Verwerkersovereenkomst, geldt Verwerker als Verwerkingsverantwoordelijke als hij zonder inhoudelijke tussenkomst van Verwerkingsverantwoordelijke beslist tot inzage in of Verstrekking van Persoonsgegevens aan een toezichthouder of overheidsinstantie

Artikel 11. Rechten van Betrokkene

11.1 Verwerker zal zijn volledige medewerking verlenen opdat Verwerkingsverantwoordelijke kan voldoen aan zijn wettelijke verplichtingen in het geval dat een Betrokkene zijn rechten uitoefent

op grond van hoofdstuk 3 (vanaf artikel 12 e.v.) van de AVG of andere toepasselijke regelgeving betreffende de Verwerking van Persoonsgegevens. Wanneer Verwerkingsverantwoordelijke een verzoek van een Betrokkene ontvangt ten aanzien van het uitoefenen van zijn of haar rechten, dan werkt Verwerker daar binnen een termijn van 14 dagen aan mee.

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

Artikel 12. Wijziging Verwerkersovereenkomst

12.1 Indien een wijziging in relevante wet- en/of regelgeving, in de te verwerken Persoonsgegevens of een risicoanalyse van de Verwerking van Persoonsgegevens daartoe aanleiding geeft zullen Partijen de Verwerkersovereenkomst wijzigen.

12.2 Wijziging van deze Verwerkersovereenkomst kan slechts schriftelijk plaatsvinden door middel van een door beide Partijen ondertekend addendum.

12.3 De wijzigingen kunnen nooit tot gevolg hebben dat Verwerkingsverantwoordelijke niet kan voldoen aan de AVG en overige relevante wet- en regelgeving met betrekking tot Persoonsgegevens.

Artikel 13. Aansprakelijkheid

13.1 Indien de Verwerker tekort schiet in de nakoming van de verplichtingen uit deze Verwerkersovereenkomst kan de Verwerkingsverantwoordelijke hem in gebreke stellen. Verwerker is echter onmiddellijk in verzuim als de nakoming van desbetreffende verplichting anders dan door overmacht binnen de overeengekomen termijn, reeds blijvend onmogelijk is. Ingebrekestelling geschiedt schriftelijk, waarbij aan de Verwerker een redelijke termijn wordt gegund om alsnog zijn verplichtingen na te komen. Deze termijn is een fatale termijn. Indien nakoming binnen deze termijn uitblijft, is Verwerker in verzuim.

13.2 Verwerker is aansprakelijk voor alle schade ~~of nadeel~~ voortvloeiende uit het niet-nakomen van, of in strijd handelen met de bij of krachtens de AVG, gegeven voorschriften en/of het niet-nakomen van, of in strijd handelen met het in deze Verwerkersovereenkomst bepaalde, onverminderd de aanspraken op grond van wettelijke regels. Verwerker is aansprakelijk voor schade ~~of nadeel~~ voor zover ontstaan door zijn werkzaamheid of die van door hem ingeschakelde Onderaannemers (Derden). Verwerker is tevens aansprakelijk voor alle schade ~~of nadeel~~ voortvloeiende uit de door zijn werkzaamheid ontstane inbreuken op de persoonlijke levenssfeer van Betrokkenen.

13.3 De in het tweede lid bedoelde aansprakelijkheid voor persoons- en zaakschade en daaruit voortvloeiende schade, is beperkt tot een bedrag van € 1.250.000,– per gebeurtenis. Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis.

~~13.2~~13.4 De aansprakelijkheid voor overige schade is beperkt tot tien maal de jaarvergoeding per gebeurtenis. De totale aansprakelijkheid per jaar bedraagt evenwel nooit meer dan twintig maal de jaarvergoeding (ongeacht het aantal gebeurtenissen). Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis.

~~13.3~~13.5 Indien Verwerker enige in de AVG genoemde verplichting niet nakomt, en er worden aan de Verwerkingsverantwoordelijke in verband hiermee (een) boetes opgelegd door bijvoorbeeld de Autoriteit Persoonsgegevens, is Verwerker een vergoeding verschuldigd aan de Verwerkingsverantwoordelijke, even groot als de aan Verwerkingsverantwoordelijke ter zake opgelegde boete, zonder dat hiervoor een aanmaning of een voorafgaande verklaring nodig is. Deze vergoeding is niet vatbaar voor verrekening en opschorting en laat het recht van

Verwerkingsverantwoordelijke op nakoming en schadevergoeding onverlet. Tevens heeft de Verwerkingsverantwoordelijke het recht om de Overeenkomst in bovengenoemde situatie met onmiddellijke ingang op te zeggen zonder dat de Verwerker aanspraak kan maken op enige vorm van schadevergoeding. Mocht de oplegging van de boete om welke reden dan ook worden teruggedraaid en heeft Verwerker deze boete reeds vergoed aan Verwerkingsverantwoordelijke, dan zal Verwerkingsverantwoordelijke de vergoeding onverwijld aan Verwerker terugbetalen, zodra Verwerkingsverantwoordelijke het bedrag retour heeft ontvangen van de opleggende partij.

~~13.4 Beperkingen van de in dit artikel genoemde aansprakelijkheid in onderliggende Overeenkomst, zoals bedoeld in 1.12, zijn uitgesloten.~~

Artikel 14. (Intellectuele) eigendomsrechten en zeggenschap

14.1 Alle (intellectuele) eigendomsrechten - daaronder begrepen enig auteursrecht en databankenrecht - op (het Bestand c.q. de Bestanden van) gegevens, data, informatie en enig ander materiaal of content die de Verwerkingsverantwoordelijke en/of Gebruikers invoeren, versturen, plaatsen of anderszins verwerken met behulp van de Dienst blijven te allen tijde berusten bij Verwerkingsverantwoordelijke, de betreffende Gebruiker, dan wel hun respectievelijke licentiegever(s).

14.2 Verwerker heeft geen zelfstandige zeggenschap over bovengenoemde informatie die door hem worden Verwerkt. De zeggenschap berust bij Verwerkingsverantwoordelijke en/of de betreffende Gebruiker.

Artikel 15. Toepasselijk recht en bevoegde rechter

15.1 Op deze Verwerkersovereenkomst en op alle geschillen die daaruit mogen voortvloeien of daarmee mogen samenhangen, is het Nederlands recht van toepassing.

15.2 Alle geschillen, welke tussen Partijen mochten ontstaan in verband met de Verwerkersovereenkomst, zullen worden voorgelegd aan de Rechtbank Utrecht

Aldus overeengekomen en in tweevoud opgemaakt.

Verwerkingsverantwoordelijke **Verwerker**

Utrecht, [DATUM]

_____
A. van Vuuren
Directeur

Plaats, [DATUM]

_____
Naam
Functie

Bijlage A: specificatie verwerking Persoonsgegevens

Deze bijlage specificeert de persoonsgegevens die namens Verwerkingsverantwoordelijke door Verwerker worden verwerkt, definieert het doel van deze verwerking, beschrijft de door Verwerker getroffen beveiligingsmaatregelen, en benoemt de Onderaannemers die Verwerker inzet bij de uitvoering van de Dienst.

A.1 Verwerkingsactivitetiten

Verwerkingsverantwoordelijke laat Persoonsgegevens door Verwerker verwerken omdat Verwerkingsverantwoordelijke gebruik wil maken van de Dienst "***" van Verwerker. Met behulp van deze Dienst kan Verwerkingsverantwoordelijke invullen geven aan de taak "***".

A.2 Categorieën Betrokkenen

De Persoonsgegevens die in het kader van deze Verwerkersovereenkomst worden uitgewisseld, hebben betrokken op de hieronder opgesomde Betrokkenen.

1. Medewerkers (dienstverband en inhuur) van Omgevingsdienst regio Utrecht (ODRU);
2. Burgers (natuurlijke personen) van o.a. de volgende gemeenten:
    a. Gemeente Bunnik
    b. Gemeente De Bilt
    c. Gemeente Montfoort
    d. Gemeente Oudewater
    e. Gemeente Renswoude
    f. Gemeente Rhenen
    g. Gemeente De Ronde Venen
    h. Gemeente Stichtse Vecht
    i. Gemeente Utrechtse Heuvelrug
    j. Gemeente Veenendaal
    k. Gemeente Vijfheerenlanden
    l. Gemeente Woerden
    m. Gemeente Wijk bij Duurstede
    n. Gemeente IJsselstein
    o. Gemeente Zeist
3. Medewerkers (natuurlijke personen) van de volgende gemeenten:
    a. Gemeente Bunnik
    b. Gemeente De Bilt
    c. Gemeente Montfoort
    d. Gemeente Oudewater
    e. Gemeente Renswoude
    f. Gemeente Rhenen
    g. Gemeente De Ronde Venen
    h. Gemeente Stichtse Vecht
    i. Gemeente Utrechtse Heuvelrug
    j. Gemeente Veenendaal
    k. Gemeente Vijfheerenlanden
    l. Gemeente Woerden
    m. Gemeente Wijk bij Duurstede
    n. Gemeente IJsselstein
    o. Gemeente Zeist

A.3 De te verwerken Persoonsgegevens, doeleinden gegevensverwerking en bewaartermijnen
De onderstaande tabel toont de Persoonsgegevens die Verwerker namens Verwerkingsverantwoordelijke verwerkt, het doel van de verwerking en de bewaartermijnen. Het gaat niet enkel om Persoonsgegevens die Verwerkingsverantwoordelijke direct aan Verwerker verstrekt, maar ook om Persoonsgegevens die Gebruiker aanlevert bij gebruik van de ter beschikking gestelde faciliteiten (de Dienst).

Categorie Betrokkene	**Persoonsgegevens**	**Doeleinde**	**Bewaartermijn**

A.4 Beveiligingsnorm
De Verwerker hanteert voort informatiebeveiliging de volgende norm (kruis aan wat van toepassing is)
☐ ISO norm 27001
☐ NEN 7510
☐ Baseline Informatiebeveiliging Overheid (BIO)
☐ ISAE 3402, namelijk type: _____
☐ Anders, namelijk _____

De Verwerker toont de toereikendheid van informatiebeveiliging aan middels (kruis aan wat van toepassing is):

☐ Certificering, inclusief Verklaring van Toepasselijkheid;

Naam certificaat	**Organisatieonderdeel/ dienst waarop certificaat betrekking heeft**	**Geldigheidsduur certificaat**	**Verklaring van toepasselijkheid**

☐ Derdenverklaring / TPM (Third Party Memorandum)

Naam derdenverklaring / TPM	**Organisatieonderdeel/ dienst waarop het betrekking heeft**	**Geldigheidsduur**

☐ Anders, namelijk _____

A.5 Getroffen beveiligingsmaatregelen
De door Verwerker getroffen beveiligingsmaatregelen betreffen in ieder geval de maatregelen die zijn beschreven in de bijgevoegde en door Verwerker ondertekende Bijlage C: Richtlijn beveiligingsafspraken derden.

Indien van toepassing wordt ook door Verwerker aan Verwerkingsverantwoordelijke ter hand gestelde beveiligingsdocumentatie of (audit / assurance) rapporten toegevoegd aan deze Verwerkersovereenkomst voor zover deze geen onderdeel zijn van de Overeenkomst zoals bedoeld in 1.12.

A.6 Onderaannemers
Verwerker heeft toestemming van Verwerkingsverantwoordelijke om de volgende Onderaannemers in te zetten bij de uitvoering van de Dienst:

Naam organisatie: [NAAM]
- Korte omschrijving dienstverlening
  (v) [INVULLEN]
- Mate van Verwerking Persoonsgegevens
  (vi) [INVULLEN]
- Plaats/Land van Verwerking Persoonsgegevens
  (vii) [INVULLEN]

Naam organisatie: [NAAM]
- Korte omschrijving dienstverlening
  (viii) [INVULLEN]
- Mate van Verwerking Persoonsgegevens
  (ix) [INVULLEN]
- Plaats/Land van Verwerking Persoonsgegevens
  (x) [INVULLEN]

Indien na ondertekening van deze overeenkomst een Onderaannemer wordt ingeschakeld dan moet Verwerker hier expliciet toestemming voor vragen en verkrijgen van Verwerkingsverantwoordelijke.

A.7 Categorieën medewerkers die persoonsgegevens verwerken
Verwerker verschaft alleen (ingehuurde) medewerkers die het voor het uitvoeren van hun functie nodig hebben toegang tot de Persoonsgegevens. De volgende categorieën medewerkers hebben toegang tot de Persoonsgegevens:

[Invullen]

A.8 Contactgegevens
Bij vragen over deze Bijlage en/of de geleverde Dienst, kan contact worden opgenomen met:

Naam: *** (Verwerkingsverantwoordelijke)
Functie: ***
E-mailadres: ***
Telefoonnummer: ***

Naam: *** (Verwerker)
Functie: ***
E-mailadres: ***
Telefoonnummer: ***

Voor het melden van een Datalek als bedoeld in artikel 6 kan contact worden opgenomen met:

Naam: (Verwerkingsverantwoordelijke)
Functie: Functionaris gegevensbescherming
E-mailadres: privacy@odru.nl
Telefoonnummer:

Naam: *** (Verwerker)
Functie: ***
E-mailadres: ***
Telefoonnummer: ***

Verwerkingsverantwoordelijke	**Verwerker**
Utrecht, [DATUM]	Plaats, [DATUM]
_____	_____
A. van Vuuren	Naam
Directeur	Functie

Bijlage B: Informatie die moet worden verstrekt bij een Datalek

Als Verwerker de Verwerkingsverantwoordelijke moet informeren op grond van artikel 6, zal hij minimaal de volgende gegevens moeten verschaffen:

Contactgegevens melder
[NAAM, FUNCTIE, EMAILADRES, TELEFOONNUMMER]

Gegevens over het Datalek

- Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van (Persoons)gegevens zich heeft voorgedaanVond het Datalek plaats bij de Verwerker of de Onderaannemer?
- Welke typen (bijzondere) Persoonsgegevens zijn betrokken bij het Datalek?
- Van hoeveel personen zijn de Persoonsgegevens betrokken bij het Datalek? Geef a.u.b. een minimum en maximum aantal personen.
- Omschrijving groep personen om wiens gegevens het gaat.
- Wat is de oorzaak van het beveiligingsincident?
- Periode van het Datalek:
    - Startdatum van de periode waarbinnen de inbreuk was
    - Einddatum van de periode waarbinnen de inbreuk was
    - Datum waarop de inbreuk werd ontdekt

Vervolgacties naar aanleiding van het Datalek

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

Verwerkingsverantwoordelijke	**Verwerker**
Utrecht, [DATUM]	Plaats, [DATUM]
_____	_____
A. van Vuuren	Naam
Directeur	Functie

Bijlage C: Richtlijn beveiligingsafspraken derden

C.1 Inleiding

Om de veiligheid van bedrijfsapplicaties en de hierin verwerkte gegevens te kunnen waarborgen, is het van belang dat informatiesystemen voldoen aan binnen de Omgevingsdienst regio Utrecht (ODRU) geldende beveiligingseisen. Dit geldt zowel voor intern gehoste applicaties, als voor (web)applicaties die extern zijn ondergebracht. In dit document zijn uitgangspunten opgenomen waaraan diensten van derden aan dienen te voldoen.

Door dit document standaard als bijlage toe te voegen aan relevante overeenkomsten met derden, borgt de ODRU dat er goede afspraken worden gemaakt op het gebied van informatiebeveiliging (in lijn met de eisen uit de Baseline Informatiebeveiliging Overheid en de AVG). Dit voorkomt niet alleen onnodige discussies in de praktijk, maar maakt ook aantoonbaar dat de ODRU haar wettelijke verantwoordelijkheid neemt. De wet stelt namelijk dat de ODRU ook verantwoordelijk is voor de beveiliging van haar informatie bij leveranciers en partners. Werkzaamheden kunnen worden uitbesteed, maar verantwoordelijkheden niet.

Gebruik

Het gebruik van dit document is verplicht en vormt in de praktijk aanleiding om met leveranciers specifieke afspraken te maken ten aanzien van de informatiebeveiliging van de beoogde af te nemen middelen en/of diensten. De CISO, FG en Adviseur Informatiebeveiliging & Privacy hebben gedurende het verlengings- of inkooptraject (voorafgaand aan het definitief aangaan van een overeenkomst) contact met de leverancier(s) over de in dit document beschreven beveiligingsuitgangspunten.

Samen met de leverancier(s) wordt vastgesteld welke onderdelen uit deze richtlijn mogelijk niet van toepassing zijn, en op welke punten er wordt afgeweken van de beschreven uitgangspunten. Eventuele acceptabele afwijkingen worden door de CISO, FG en Adviseur Informatiebeveiliging & Privacy voorafgaand aan ondertekening verwerkt in hoofdstuk C.3 van deze richtlijn. Vervolgens wordt voorliggend document inclusief een eventuele bijlage met afwijkingen, toegevoegd als bijlage bij de verwerkersovereenkomst.

Wanneer de CISO, FG en Adviseur Informatiebeveiliging & Privacy constateren dat de informatiebeveiliging van de leverancier onvoldoende is, dan wordt het aangaan van een overeenkomst uitgesteld tot het moment dat de leverancier wèl aan de beveiligingseisen van de ODRU voldoet.

Definities

Met “(interne) gebruikers/beheerders” worden niet alleen gebruikers/beheerders van de ODRU bedoeld (intern), maar ook gebruikers/beheerders aan de leveranciers zijde.

Met “relaties” worden doorgaans externe gebruikers (geen medewerkers van de ODRU) van een (web)applicatie bedoeld. Dit kunnen bijvoorbeeld klanten of partners zijn, maar ook burgers of consumenten.

C.2 Uitgangspunten

Versleuteling

ID	Uitgangspunt
RBD1	De netwerkverbinding tussen het werkstation van de (interne) gebruikers/beheerders en de (web)applicatie is beveiligd met adequate versleuteling[1].
	Een versleutelde verbinding tussen gebruikers en de (web)applicatie voorkomt dat de authenticatiegegevens van gebruikers misbruikt kunnen worden en de vertrouwelijkheid en integriteit van door de applicatie verwerkte gegevens tijdens het transport kan worden gecompromitteerd.
RBD2	Indien er vertrouwelijke gegevens worden uitgewisseld dan is de netwerkverbinding tussen relaties (klanten/partners) en de (web)applicatie adequaat versleuteld[1].
	Gezien het openbare karakter van internet dienen vertrouwelijke gegevens beschermd te zijn tegen misbruik. Over het algemeen wordt dit gerealiseerd middels het aanbrengen van een beveiligingscertificaat. De pagina's waarop vertrouwelijke gegevens worden uitgewisseld dienen vervolgens alleen via het versleutelde kanaal benaderbaar te zijn.
RBD3	Indien de (web)applicatie gegevens uitwisselt met externe systemen, dan is deze gegevensuitwisseling adequaat versleuteld[1].
	Onveilige gegevensuitwisseling stelt gebruikers van externe netwerken mogelijk in staat om de integriteit en vertrouwelijkheid van de gegevens te compromitteren. Gegevens die de primaire hostingomgeving verlaten worden daarom tijdens het transport versleuteld en opgeslagen op een systeem dat van goede authenticatie- en autorisatiemaatregelen is voorzien.

Logische toegangsbeveiliging

ID	Uitgangspunt
RBD4	Gebruikers/beheerders zijn in staat om zelf hun wachtwoord te wijzigen.
	Indien gebruikers binnen de applicatie niet zelf hun wachtwoord kunnen wijzigen, zal dit wachtwoord altijd bekend zijn/blijven bij de medewerker die het wachtwoord heeft aangemaakt.
RBD5	Voor beheerders en interne gebruikers wordt het wachtwoordbeleid van de ODRU[2] binnen de applicatie technisch afgedwongen.
	Door technisch de wachtwoordpolicy af te dwingen, wordt gegarandeerd dat gebruikers de voor hen toegankelijke gegevens adequaat beschermen. Eenvoudige wachtwoorden worden voorkomen. Indien een onbevoegd persoon in het bezit is gekomen van een gebruikerswachtwoord, is de periode dat hij/zij dit wachtwoord onterecht kan gebruiken beperkt. Ook dient multi-factor authenticatie te worden overwogen.
RBD6	Relaties van de ODRU (klanten, partners) wordt bij het kiezen van een wachtwoord getoond of een wachtwoord zwak, gemiddeld of krachtig is. Het kiezen van een sterk wachtwoord is de verantwoordelijkheid van de relatie. Zolang relaties enkel toegang hebben tot hun eigen gegevens, wordt technisch niet afgedwongen dat wachtwoorden van relaties aan het wachtwoordbeleid van de ODRU[2] voldoen.
	Relaties verplichten om voor de bescherming van hun eigen gegevens een sterk wachtwoord te kiezen (en te onthouden) is een vrij zware maatregel die tot ergernis kan

[1] Tot adequate versleuteling behoren onder andere technieken zoals TLS of IPSEC. Voor de configuratie van TLS verbindingen is de richtlijn van het NCSC leidend. Voor andere encryptietechnieken zijn de sleutellengten van de BSI Recommendations (2017) op keylength.com leidend.

[2] Wachtwoorden zijn minimaal 14 tekens lang en mogen bestaan uit uitsluitend kleine letters. De geldigheid is maximaal 91 dagen en hergebruik van laatste 10 wachtwoorden is niet toegestaan. Na 4 foutieve inlogpogingen binnen een periode van 30 minuten wordt het account voor 30 minuten geblokkeerd.

	leiden. Door aan te geven wat de kracht van een gekozen wachtwoord is voldoen we aan onze zorgplicht en verleggen we aantoonbaar de verantwoordelijkheid rondom de keuze voor een goed wachtwoord naar de gebruiker.
RBD7	Wachtwoorden worden op het systeem en/of in een database nooit in leesbare vorm opgeslagen. In plaats daarvan wordt een hash (éénrichtingsversleuteling) van het wachtwoord vastgelegd om de authenticatie uit te kunnen voeren.
	Door een gehashte variant van een wachtwoord op te slaan, wordt de impact van data diefstal beperkt. Een aanvaller die via een computerinbraak wachtwoordhashes weet buit te maken zal deze hashes moeten kraken voordat deze bruikbaar zijn. Gebruik een dynamisch gesalte hash om te voorkomen dat wachtwoord/hash combinaties van het hashtype eenvoudig voorberekend kunnen worden in wachtwoordtabellen.
RBD8	Indien webapplicaties communiceren met databases of externe systemen dan zijn de hiervoor gebruikte (service-)accounts voorzien van een sterk en uniek wachtwoord.
	Indien een applicatie gebruik maakt van standaard accounts en wachtwoorden, dan zijn andere klanten van de leverancier mogelijk in staat om toegang te krijgen tot de gegevens van de ODRU. Bijvoorbeeld wanneer deze toegang hebben tot het LAN van de ODRU. Ook een aanvaller die een dergelijk wachtwoord elders wist te bemachtigen, kan op deze manier makkelijker toegang krijgen tot gegevens. Dit wordt voorkomen door unieke en sterke wachtwoorden te gebruiken die voldoen aan het wachtwoordbeleid van de ODRU[3].
RBD9	De applicatie beschikt over mogelijkheden om rollen voor applicatiegebruikers aan te maken die toegang hebben tot exact de juiste applicatieonderdelen. Gebruikers/beheerders worden voorzien van de juiste rechten (niet teveel, niet te weinig) die nodig zijn voor uitoefening van de functie.
	Door gebruikers een rol toe te kennen met exact de juiste functionaliteit, wordt voorkomen dat gebruikers toegang hebben tot overbodige (vertrouwelijke) informatie.
RBD10	Indien een applicatie voor databasetoegang of andere backoffice systemen een generiek (dus geen eindgebruiker-specifiek) account inzet, dan zijn de rechten van dit account zoveel mogelijk beperkt.
	Door de rechten van accounts zoveel mogelijk te beperken wordt de kans op een datalek beperkt. Door applicaties alleen rechten te geven tot hun eigen databases en databasetabellen, wordt voorkomen dat kwetsbaarheden in applicatie A via de database gevolgen kunnen hebben voor de applicaties B en C. In het geval van shared hosting wordt hiermee ook voorkomen dat accounts van een andere klant van de leverancier toegang hebben tot gegevens van de ODRU.
~~RBD11~~	~~Applicaties / applicatieonderdelen die alleen door medewerkers/beheerders worden gebruikt, zijn alleen vanaf specifiek benoemde IP-adressen toegankelijk.~~
	~~Door met IP filtering en/of een VPN koppeling te voorkomen dat elke internetgebruiker de applicatie van de ODRU kan benaderen, wordt preventief de kans verkleind dat een aanvaller succesvol een wachtwoord raad of misbruik maakt van een (web)applicatiefout.~~
RBD12	Back-ups waarop vertrouwelijke data aanwezig is zijn fysiek (tijdens opslag) en logisch (tijdens transport) dusdanig beschermd dat enkel geautoriseerde beheerders toegang tot deze back-ups hebben.
	De back-ups bevatten dezelfde gegevens als op de server aanwezig zijn en dienen daarom goed beschermd te worden. Back-ups die een beveiligde locatie verlaten zijn daarom versleuteld.
RBD13	Indien vertrouwelijke data voor test- of ontwikkeldoeleinden voor medewerkers toegankelijk moet zijn die geen productiefunctie vervullen, dan is deze data geanonimiseerd.

[3] Wachtwoorden van service accounts bestaan uit een willekeurige reeks tekens van minimaal 20 karakters, en kennen een onbeperkte geldigheid.

	Met het beperken van toegang tot vertrouwelijke data wordt misbruik van deze data voorkomen.

Patchmanagement

ID	Uitgangspunt
RBD14	De gehele (web)omgeving is en blijft voorzien van de laatste security updates en er wordt geen gebruik gemaakt van end-of-life (EOL) software.
	Security updates van software zijn essentieel om de integriteit, vertrouwelijkheid en beschikbaarheid van het platform / de dienst te kunnen blijven garanderen. Een groot deel van misbruik door aanvallers, is het gevolg van kwetsbaarheden waar reeds patches voor beschikbaar waren. Onder software wordt onder andere verstaan: besturingssysteem, webserver-, applicatie- en databasesoftware, maar ook firmware van appliances zoals loadbalancers, switches en firewalls.

Hardening

ID	Uitgangspunt
RBD15	De applicatie toont gebruikers geen gedetailleerde (systeem technische) foutmeldingen.
	Door gebruikers in een foutsituatie enkel te voorzien van algemene informatie aan de hand waarvan de helpdesk actie kan ondernemen, wordt voorkomen dat aanvallers door het bewust creëren van foutsituaties in het bezit komen van systeemtechnische informatie.
RBD16	Indien een server waarop een website of database van de ODRU wordt gehost, gebruikt wordt voor het hosten van meerdere websites, dan garandeert de leverancier dat het voor de beheerders van de overige websites onmogelijk is om toegang te verkrijgen tot de broncode van de website van de ODRU of de inhoud van de aan de ODRU toegekende database(tabellen).
	Alleen gebruikers en beheerders van de ODRU dienen de mogelijkheid te hebben data van de ODRU te bevragen.
RBD17	Op het besturingssysteem, de webserver, de applicatieserver en de databaseserver die gebruikt worden voor het hosten van de applicatie is alleen de hoogst noodzakelijke functionaliteit actief.
	Overbodige functionaliteit kan fouten bevatten en daarmee een onnodig risico vormen voor de webomgeving. Een grondige hardening van de omgeving voorkomt dit.

Netwerkbeveiliging

ID	Uitgangspunt
RBD18	De webserver wordt middels een stateful firewall beschermd tegen netwerkgebaseerde aanvallen vanaf internet. Alleen de voor de applicatie noodzakelijke diensten zijn benaderbaar voor alle internet gebruikers.
	Toegang tot overbodige services verhoogt het risicoprofiel van de webserver onnodig.

Veilig ontwikkelen

ID	Uitgangspunt
RBD19	De (web)applicatie bevat geen kwetsbaarheden zoals beschreven in de OWASP Top 10[4]. Ontwikkelaars houden zich aan de OWASP ontwikkelprincipes en kennen de OWASP development Guide[5].
	OWASP (Open Web Application Security Project) is een open non-profit organisatie van vrijwillige experts over de hele wereld, die zich bezig houden met het begrijpen en verbeteren van de veiligheid van webapplicaties en andere webdiensten. OWASP biedt als het ware een industrieconsensus m.b.t. webapplicatiebeveiliging. Ontwikkelaars dienen tijdens de bouw van de website rekening te houden met de ontwikkelprincipes. Daarnaast moet geborgd zijn dat applicaties vrij zijn van in de OWASP Top 10 beschreven webapplicatiefouten.

Besturing van informatiebeveiliging

ID	Uitgangspunt
RBD20	De leverancier bestuurt de beveiliging van de hosting, de beveiliging van het beheer van de hosting, en de gegevens van de ODRU conform een beveiligingsmanagementsysteem (ISMS) waarin minimaal de relevante onderdelen uit de ISO 27002 zijn opgenomen. De dienstverlening van de leverancier is bepalend voor welke onderdelen uit de ISO 27002 relevant zijn, en het oordeel hierover ligt bij de Information Security Officer van de ODRU.
	De hostingprovider neemt informatiebeveiliging serieus en voert een proactief beleid om beveiligingsrisico's snel te kunnen signaleren en verhelpen. Een ISMS (ISO 27001 of vergelijkbaar) beschrijft hoe een organisatie aantoonbaar borgt dat haar informatiebeveiliging actueel en doeltreffend blijft. Vanuit dit proces voor de beheersing van informatiebeveiligingsrisico's, zijn maatregelen geselecteerd (ISO 27002) waarmee het risico tot een acceptabel niveau wordt verlaagd.

Logging en monitoring

ID	Uitgangspunt
RBD21	De systemen zijn gekoppeld aan een centrale tijdsbron van maximaal stratum 5. Het gebruik van een NTP-configuratie op basis van minimaal 3 onafhankelijke tijdservers is aan te raden.
	Om accurate tijdstippen in log- en transactiegegevens te kunnen garanderen is het belangrijk dat de systeemtijd juist is.
RBD22	Systeem- en applicatielogs worden minimaal 6 maanden bewaard en dusdanig opgeslagen dat hun integriteit na een systeeminbraak is gewaarborgd.
	De juistheid van loggegevens is belangrijk om de oorzaak van een systeeminbraak te kunnen achterhalen.
RBD23	Het detailniveau van logs is voldoende groot om bij aanvallen de handelswijze en netwerkidentiteit van de aanvaller te achterhalen.
	Het detailniveau van loggegevens is belangrijk om de oorzaak van een systeeminbraak te kunnen achterhalen. Denk bijvoorbeeld aan datum, tijd, client IP, user agent string, bytes received, bytes send, en URL.
RBD24	Kritieke systeemfuncties worden gemonitord. De alarmering van de monitoring sluit aan op de beschikbaarheidsafspraken en het daar van afgeleide servicevenster.

[4] Zie ook: https://storage.googleapis.com/google-code-archive-downloads/v2/code.google.com/owasptop10/OWASP%20Top%2010%20-%202013.pdf
[5] Zie ook: https://github.com/OWASP/DevGuide/tree/2.0.1/DevGuide2.0.1

	Monitoring helpt om problemen te signaleren en tijdig met een oplossing te kunnen komen zodat de beschikbaarheidsgaranties kunnen worden waargemaakt.

Veilig beheer

ID	Uitgangspunt
RBD25	Beheerwerkzaamheden worden uitgevoerd vanaf beveiligde beheerstations. Deze stations bevatten alleen goedgekeurde software, bevatten sterke wachtwoorden, bevatten bijgewerkte antivirus software en zijn voorzien van de laatste beveiligingsupdates. Dit laatste geldt voor alle programmatuur, dus besturingssysteem en applicatiesoftware zoals Java, Acrobat, Flash, Quicktime, enzovoorts. De harde schijven van mobiele beheerwerkplekken zijn volledig versleuteld.
	Aangezien de beheerwerkplek toegang geeft tot de systemen met data van de ODRU, is de betrouwbaarheid van deze werkplek essentieel.
RBD26	Vanaf een publieke netwerklocatie (internet) is de beheeromgeving enkel benaderbaar nadat een beheerder zich via multi-factor authenticatie heeft geïdentificeerd.
	Via Phishing is het relatief eenvoudig om gebruikers/beheerders over te halen om hun wachtwoord ergens in te tikken. Een hacker die er in slaagt het wachtwoord van een beheerder te achterhalen kan hiermee netwerkrechten tot de beheeromgeving verkrijgen. Sterke authenticatie (inloggen met een token & een wachtwoord) biedt hier bescherming tegen.
RBD27	Er is een backup- en restoreplan uitgewerkt en getest.
	Een goede backup en restore voorziening voorkomt dat verstoringen tot onacceptabel dataverlies leiden. Denk bijvoorbeeld aan cryptovirussen die niet alleen de lokale machine, maar ook het netwerk afzoeken op te versleutelen data.
RBD28	Het informatiesysteem is beschreven, de bedieningsprocedures zijn opgesteld en de configuratie is gedocumenteerd.
	Goede documentatie helpt een betrouwbare exploitatie van het platform te waarborgen.
RBD29	Op productiesystemen zijn geen ontwikkeltools, testhulpmiddelen of broncode aanwezig.
	Met een goede scheiding tussen productie en ontwikkel-/testsystemen wordt de kans op productieverstoringen kleiner. Daarnaast vergroten ontwikkeltools, testhulpmiddelen of broncode de mogelijkheden die een aanvaller heeft om misbruik van een productiesysteem te maken.
RBD30	De leverancier werkt met betrouwbaar beheerpersoneel, bijvoorbeeld door bij aanname van nieuw personeel de referenties te controleren en/of een Verklaring Omtrent het Gedrag (VOG[6]) aan te vragen.
	De systeemrechten die aan beheerpersoneel zijn toegekend geven toegang tot (vertrouwelijke) data van de ODRU. De kans op fraude door personeel dient te worden beperkt.
RBD31	Beheerpersoneel (of ander personeel met toegang tot gegevens van de ODRU) heeft een verklaring ondertekend die de geheimhouding van gegevens van de ODRU afdwingt. Daarnaast beschrijft de verklaring de sancties die van toepassing zijn indien de geheimhoudingsplicht niet wordt nageleefd.
	Een geheimhoudingsverklaring helpt misbruik van vertrouwelijke gegevens van de ODRU te voorkomen.

[6] https://www.justis.nl/producten/vog/

Mobiele applicaties (apps)

ID	Uitgangspunt
RBD32	Indien er vanuit een app een TLS verbinding wordt opgezet, beschermt de app tegen zogenaamde man-in-the-middle aanvallen.
	De app controleert de integriteit van een TLS verbinding voordat deze wordt opgezet. Dit kan bijvoorbeeld door een strikte controle op server certificaten uit te voeren via certificate pinning[7].
RBD33	Indien een app vertrouwelijke data op het mobiele device opslaat (zoals persoonsgegevens), dan wordt deze data op een veilige plek versleuteld opgeslagen.
	IOS biedt de mogelijkheid om data op te slaan binnen een versleuteld deel van de IOS keychain. Binnen Android kan gebruik worden gemaakt van versleutelde opslag binnen een specifiek aan de app toegewezen data directory.
RBD34	Indien er binnen de app gebruik wordt gemaakt van een analytics provider, dan wordt deze provider in overleg met de ODRU gekozen.
	Ook met de analytics provider zullen afspraken rondom privacy en beveiliging gemaakt moeten worden.
RBD35	Indien een app verbinding maakt met een webservice van waaruit persoonlijke gegevens, profielen of betaalde content wordt aangeboden, dan biedt deze webservice krachtige authenticatie en autorisatie waarborgen.
	Authenticatiegegevens mogen niet voorspelbaar zijn, maar dienen te voldoen aan het wachtwoordbeleid van de ODRU[8]. Autorisaties dienen zo te zijn ingericht dat een service de gebruiker nooit meer gegevens kan leveren dan waarvoor zijn inlogsessie geautoriseerd is.
RBD36	Kritieke beveiligingsmaatregelen worden nooit enkel client-side binnen de app geïmplementeerd, maar altijd server-side op een webserver (bijvoorbeeld binnen een webservice).
	Bij de ontwikkeling van de app houdt de ontwikkelaar er rekening mee dat een app, anders dan een website, een client-side applicatie betreft. Software welke geïnstalleerd is op apparatuur die onder controle is van een derde, kan door deze derde gemanipuleerd worden. Deze manipulatiemogelijkheden kunnen ook van invloed zijn op de webservice. Binnen webservices dient er rekening mee te worden gehouden dat aanvallers andere data aanbieden dan dat vanuit de betreffende app gebruikelijk is (input validatie).
RBD37	De app-ontwikkelaars zijn bekend met de OWASP Top 10 voor mobiele apps en passen actief maatregelen toe om misbruik via de hier beschreven bedreigingen te voorkomen.
	Naast de OWASP Top 10 voor webapplicaties, biedt OWASP ook een Top 10 voor mobiele applicaties. Ontwikkelaars dienen te borgen dat apps vrij zijn van de in OWASP Top 10 beschreven mobiele applicatiefouten.
RBD38	De app vraagt op het smartdevice geen onnodige toegang tot resources zoals de camera, microfoon, locatie, telefoon, contacten en foto's indien dit niet noodzakelijk is voor het goed functioneren van de app. De app blijft waar mogelijk (op onderdelen) functioneren indien de gebruiker besluit om de toegang tot resources weer in te trekken.
	Om de privacy van eindgebruikers zo goed als mogelijk te borgen, vraagt de app geen onnodige toegang. Instanties zoals de Autoriteit Persoonsgegevens controleren hier actief op.

[7] https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning

[8] Wachtwoorden zijn minimaal 8 tekens lang en bestaan uit hoofdletters, kleine letters en een cijfer of speciaal teken. De geldigheid is maximaal 91 dagen en hergebruik van laatste 10 wachtwoorden is niet toegestaan. Na 4 foutieve inlogpogingen binnen een periode van 30 minuten wordt het account voor 30 minuten geblokkeerd.

Privacy

ID	Uitgangspunt
RBD39	Er vindt geen bovenmatige verstrekking van persoonsgegevens plaats.
	Binnen de externe hostingomgeving worden alleen de hoogst noodzakelijke persoonsgegevens opgeslagen. Indien een applicatie enkel de naam van een relatie nodig heeft, wordt bijvoorbeeld niet het volledige NAW record aangeleverd. Indien technisch mogelijk wordt in plaats van met detailgegevens, gewerkt met een relatienummer dat door de ODRU vanuit de eigen administratie vertaald kan worden naar een relatie.
RBD40	Indien persoonsgegevens (naam, adres, telefoon, etc.) uitgewisseld worden met een leverancier of een andere derde partij (onderaannemer), is er met deze partij voordat uitwisseling plaatsvindt een verwerkersovereenkomst afgesloten. In deze overeenkomst is opgenomen voor welk doel, welke verwerkingen uitgevoerd zullen worden en welke (gespecificeerde) gegevens hiervoor worden verstrekt.
	Het afsluiten van een verwerkersovereenkomst met derden is een verplichting die voortkomt uit de Algemene Verordening Gegevensbescherming (AVG). Het helpt de ODRU om controle te houden over de wijze waarop een derde partij met door de ODRU vergaarde persoonsgegevens omgaat. Het opstellen van een verwerkersovereenkomst kan worden gefaciliteerd door een privacy officer in samenwerking met de gegevenseigenaar.
RBD41	Indien door een systeemwijziging persoonsgegevens voor een ander doel verwerkt gaan worden dan waarvoor ze zijn verzameld, is dit vooraf afgestemd met (de privacy officer van) de ODRU.
	Het gebruiken van persoonsgegevens van relaties is aan wettelijke voorwaarden gebonden. Een privacy officer kan hierover advies geven.
RBD42	Webpagina's met persoonsgegevens zijn afgeschermd van zoekmachines.
	Door zeker te stellen dat alle persoonsgegevens binnen de website niet toegankelijk zijn voor zoekmachines (vanwege autorisaties of aan zoekmachines opgelegde beperkingen) wordt voorkomen dat deze gegevens per abuis worden geïndexeerd en wereldkundig worden gemaakt.
RBD43	Het beheer van systemen waarop persoonsgegevens zijn opgeslagen vindt plaats binnen de Europese Unie of een land met een (conform EC of CBP uitspraken) passend beschermingsniveau.
	De Europese Commissie en de Autoriteit Persoonsgegevens hebben beschreven welke landen een passend beschermingsniveau bieden ten aanzien van de verwerking van persoonsgegevens. Beheer en verwerking vanuit andere landen is, tenzij expliciet anders overeengekomen en conform beperkte in de AVG vastgelegde uitzonderingen, niet toegestaan.

Clouddiensten

ID	Uitgangspunt
RBD44	Wanneer de leverancier de gegevens van de ODRU plaatst op een platform dat fysiek buiten Nederland staat, of waarvan het eigendom berust bij en niet-Nederlandse partij (bijvoorbeeld bij het gebruik van onderaannemers en/of toeleveranciers), dan wordt dit vooraf expliciet afgestemd met de ODRU.
	Om te borgen dat (persoons)gegevens van de ODRU volledig conform de Nederlandse wet (en het daarop gebaseerde beleid van de ODRU) worden behandeld, zijn buitenlandse cloudvoorzieningen mogelijk ongeschikt. Uitwisseling vanuit Nederland naar andere EU-lidstaten is mogelijk op basis van de Nederlandse AVG. Alle EU-lidstaten hebben hun wetgeving aangepast aan de Europese privacyrichtlijn, waardoor de EU één

	rechtsgebied is bij de bescherming van persoonsgegevens. Aanbieders van Amerikaanse cloudproviders dienen t.b.v. de doorgifte van persoonsgegevens te zijn aangemeld bij het Privacy Shield programma, en als gevolg daarvan zijn opgenomen in het Privacy Shield register. Doorgifte van persoonsgegevens naar andere landen buiten de EU is alleen toegestaan wanneer er gebruik wordt gemaakt van een Europees modelcontract. In alle gevallen is een verwerkersovereenkomst verplicht.

Toetsing

ID	Uitgangspunt
RBD45	Aan het eind van het traject/project kan de ODRU besluiten een penetratietest uit te (laten) voeren met deze richtlijn als (minimale) norm. Daarnaast worden nieuwe releases en major updates (upgrades) door de ODRU op veiligheid getoetst. Indien hieruit blijkt dat het platform fouten bevat die door het volgen van de secure coding of hardening principes voorkomen hadden kunnen worden, dan worden deze fouten zonder extra kosten gecorrigeerd. Hetzelfde is van toepassing indien er (bij afronding van de implementatie of tijdens exploitatie) afwijkingen van de in dit document beschreven normen worden vastgesteld.
	Een security assessment geeft inzicht in de betrouwbaarheid van het beheer en de applicatie.
RBD46	Voorafgaand aan een penetratietest of andere vorm van toetsing door de ODRU of een door de ODRU ingehuurde partij, controleert de leverancier zelf of de (web)applicatie voldoet aan de eisen in deze richtlijn. De leverancier toont dit aan door het overleggen van een rapport of verklaring van een derde partij (Third Party Mededeling,TPM).
	Hiermee wordt voorkomen dat de ODRU (herhaaldelijk) afwijkingen constateert die de leverancier ook onder eigen regie had kunnen vinden en oplossen. Het is belangrijk dat de leverancier zelf proactief met informatiebeveiliging omgaat en niet uitsluitend het lijstje met bevindingen van de ODRU afloopt.

C.3 Overeengekomen afwijkingen

Dit hoofdstuk beschrijft op welke onderdelen uit de richtlijn er wordt afgeweken van de beschreven uitgangspunten in hoofdstuk C.2. Per afwijking wordt vastgelegd waarom er wordt afgeweken, en welke alternatieve / aanvullende maatregelen er worden genomen.

ID	Beschrijven van de afwijking

Ondertekening

Door ondertekening van deze bijlage verklaart de leverancier van de ODRU zich te conformeren aan de uitgangspunten beschreven in hoofdstuk C.2 van deze richtlijn met in acht neming van de geformuleerde afwijkingen in hoofdstuk C.3.

Verwerkingsverantwoordelijke	**Verwerker**
Utrecht, [DATUM]	Plaats, [DATUM]
_____	_____
A. van Vuuren	Naam
Directeur	Functie