VERWERKERSOVEREENKOMST

Versie	2.0
Datum	mei 2018
Auteur	D.K. Keijer

Verwerkersovereenkomst

De ondergetekenden:

1. De Regionale Uitvoeringsdienst Utrecht (RUD Utrecht), statutair gevestigd te Utrecht en kantoorhoudende aan de Archimedeslaan 6 te (3584 BA) Utrecht, geregistreerd bij de kamer van koophandel onder nummer 60444037,
   te dezen vertegenwoordigd door diens directeur de heer H. Jungen,
   hierna te noemen: Opdrachtgever,

   en

2. [naam], statutair gevestigd te [plaats] en kantoorhoudende aan [straat, postcode en plaats], geregistreerd bij de kamer van koophandel onder nummer [...], te dezen vertegenwoordigd door diens [functie] de [heer/mevrouw] [naam] hierna te noemen: Wederpartij,

   hierna gezamenlijk te noemen: Partijen,

Overwegende dat:

- Voor zover Wederpartij Persoonsgegevens verwerkt ten behoeve van Opdrachtgever in het kader van de Overeenkomst, kwalificeert Opdrachtgever krachtens artikel 4, onderdeel 7 van de Verordening als Verwerkingsverantwoordelijke en kwalificeert Wederpartij krachtens artikel 4, onderdeel 8, van de Verordening als Verwerker;
- Partijen in deze verwerkersovereenkomst als bedoeld artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Wederpartij vast te leggen.

Komen overeen:

Artikel 1. Begrippen
In deze verwerkersovereenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de volgende betekenis toe:

1.1 Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.

1.2 Derde: een ieder, niet zijnde Betrokkene, Opdrachtgever, Wederpartij, of enig persoon die onder rechtsreeks gezag van Opdrachtgever of Wederpartij gemachtigd is om Persoonsgegevens te verwerken. Als Derde is tevens aan te merken een onderaannemer die in opdracht van Wederpartij Persoonsgegevens verwerkt ter uitvoering van de door Wederpartij in de Overeenkomst te leveren dienst.

1.3 Dienst: is de onder de Overeenkomst te leveren dienst door de Wederpartij.

1.4 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

1.5 Overeenkomst: [nader te omschrijven]

1.6 Persoonsgegevens: Persoonsgegevens als bedoeld in de Verordening die Wederpartij in het kader van de Overeenkomst ten behoeve van Opdrachtgever verwerkt.

1.7 Verordening: 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 de Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

1.8 Uitvoeringswet: Uitvoeringswet Algemene verordening gegevensbescherming.

1.9 Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

1.10 Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, in opdracht van de verwerker, is een sub-verwerker.

1.11 Verwerkersovereenkomst: onderhavige overeenkomst inclusief de overwegingen en bijbehorende bijlagen. De Verwerkersovereenkomst maakt deel uit van de Overeenkomst.

1.12 Verwerking: een bewerking of een geheel van bewerkingen in het kader van de Overeenkomst met betrekking tot Persoonsgegevens, of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen.

Artikel 2. Ingangsdatum en duur

2.1 De Verwerkersovereenkomst treedt in werking op het moment waarop deze door Partijen is ondertekend.

2.2 De Verwerkersovereenkomst eindigt nadat en voor zover Wederpartij alle Persoonsgegevens overeenkomstig artikel 9.2 heeft terugbezorgd of vernietigd.

Artikel 3. Voorwerp van deze Verwerkersovereenkomst

3.1 Deze Verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Wederpartij in het kader van de Overeenkomst.

3.2 De aard en het doel van de Verwerking, het soort Persoonsgegevens en de categorieën van betrokkenen zijn in Bijlage 1, onderdeel I omschreven.

3.3 Wederpartij garandeert de toepassing van passende technische en organisatorische maatregelen, opdat de Verwerking aan de vereisten van de Verordening en Uitvoeringswet voldoet en de bescherming van de rechten van de Betrokken is gewaarborgd.

3.4 Wederpartij garandeert te voldoen aan de verplichtingen van de toepasselijke wet- en regelgeving, waaronder de Verordening en de Uitvoeringswet betreffende de verwerking van Persoonsgegevens.

Artikel 4. Verplichtingen Wederpartij

4.1 Wederpartij verwerkt gegevens ten behoeve van Opdrachtgever in overeenstemming met diens schriftelijke instructies. Wederpartij verbindt zich de verwerkingsinstructies te volgen zoals bepaald in Bijlage 1 behorend bij deze Verwerkersovereenkomst, tenzij Partijen onderling schriftelijk afwijkende afspraken maken en behoudens afwijkende wettelijke verplichtingen.

4.2 Wederpartij heeft geen zeggenschap op de ter beschikking gestelde Persoonsgegevens. Zo neemt hij geen beslissingen over ontvangst en gebruik van de Persoonsgegevens, de verstrekking van Persoonsgegevens aan Derden en de duur van de opslag van deze gegevens. De zeggenschap over de Persoonsgegevens verstrekt onder deze verwerkersovereenkomst komt nimmer bij Wederpartij te berusten.

4.3 De verwerking van Persoonsgegevens heeft tot doel de in de Overeenkomst te leveren dienst aan Opdrachtgever te verlenen. Verwerking door Wederpartij zal daarom uitsluitend plaatsvinden voor zover noodzakelijk om deze dienst te verlenen. De categorieën van Persoonsgegevens die worden verwerkt staan gespecificeerd in Bijlage 1, onderdeel III.

4.4 Wederpartij zal Persoonsgegevens die hem in het kader van de Overeenkomst ter Beschikking zijn gesteld niet langer bewaren dan noodzakelijk is voor de uitvoering van de Overeenkomst of om een op hem rustende wettelijke verplichting na te komen.

4.5 Wederpartij stelt Opdrachtgever te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de toepasselijke wet- en regelgeving, waaronder de Verordening en de Uitvoeringswet, de verwerking van Persoonsgegevens, meer in het bijzonder de rechten van Betrokkenen, zoals, maar niet beperkt tot een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens en het uitvoeren van een gehonoreerd aangetekend verzet.

Artikel 5. Geheimhoudingsplicht

5.1 Personen in dienst van, dan wel werkzaam ten behoeve van Wederpartij, evenals Wederpartij zelf, zijn verplicht tot geheimhouding met betrekking tot de Persoonsgegevens waarvan zij kennis kunnen nemen, behoudens voor zover een bij, of krachtens de wet gegeven voorschrift tot verstrekking verplicht. De medewerkers van Wederpartij tekenen hiertoe een geheimhoudingsverklaring. De geheimhoudingsverklaring wordt voor onbepaalde tijd aangegaan en is niet beperkt tot de duur van deze Verwerkersovereenkomst.

5.2 Indien Wederpartij op grond van een wettelijke verplichting gegevens dient te verstrekken, zal Wederpartij de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal Wederpartij Opdrachtgever onmiddellijk, voorafgaand aan de verstrekking, ter zake informeren, tenzij wettelijke bepalingen dit verbieden.

Artikel 6. Meldplicht datalekken en beveiligingsincidenten

6.1 Wederpartij zal Opdrachtgever zo spoedig mogelijk – doch uiterlijk binnen 24 uur na de eerste ontdekking – informeren over alle (vermoedelijke) inbreuken op de beveiliging alsmede andere incidenten die op grond van wetgeving moeten worden gemeld aan de Autoriteit Persoonsgegevens dan wel een andere daartoe bevoegde toezichthouder, of Betrokkene, onverminderd de verplichting de gevolgen van dergelijke inbreuken en incidenten zo snel mogelijk ongedaan te maken dan wel te beperken, al dan niet onder verbeurte van een boete in geval van niet-nakoming als bedoeld in artikel 10.3 van deze Verwerkersovereenkomst. Wederpartij zal voorts, op het eerste verzoek van de Opdrachtgever, alle inlichtingen verschaffen die Opdrachtgever noodzakelijk acht om de (vermoedelijke) inbreuken alsmede andere incidenten te kunnen beoordelen. Daarbij verschaft Wederpartij in ieder geval de informatie aan Opdrachtgever zoals omschreven in Bijlage 1, onderdeel V.

6.2 Wederpartij beschikt over een gedegen plan van aanpak betreffende de omgang met en afhandeling van inbreuken en zal Opdrachtgever, op diens verzoek, inzage verschaffen in het plan van aanpak. Wederpartij stelt Opdrachtgever op de hoogte van materiële wijzigingen in het plan van aanpak.

6.3 Wederpartij zal het doen van meldingen aan de Autoriteit Persoonsgegevens dan wel aan een andere daartoe bevoegde toezichthouder overlaten aan Opdrachtgever.

6.4 Wederpartij zal alle noodzakelijke medewerking verlenen aan het zo nodig, op het kortst mogelijke termijn, verschaffen van aanvullende informatie aan de Autoriteit Persoonsgegevens dan wel een ander daartoe bevoegde toezichthouder en/of Betrokkenen. Daarbij verschaft Wederpartij in ieder geval informatie, zoals beschreven in Bijlage 1, onderdeel V, aan Opdrachtgever.

6.5 Wederpartij houdt een gedetailleerd logboek bij van alle (vermoedens van) inbreuken op de beveiliging, evenals de maatregelen die in het vervolg op dergelijke inbreuken zijn genomen waarin minimaal de informatie zoals bedoeld in Bijlage 1, onderdeel V is opgenomen, en geeft daar op eerste verzoek van Opdrachtgever inzage in.

Artikel 7. Beveiligingsmaatregelen en controle

7.1 Wederpartij neemt alle passende technische en organisatorische maatregelen om de Persoonsgegevens welke worden verwerkt ten dienste van de Opdrachtgever te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze wijze van beveiliging wordt nader omschreven in Bijlage 1, onderdeel IV en Bijlage 2 "Richtlijn beveiligingsafspraken derden".

7.2 Opdrachtgever is te allen tijde gerechtigd de verwerking van Persoonsgegevens te (doen) controleren. Wederpartij is verplicht Opdrachtgever, de Autoriteit Persoonsgegevens dan wel een andere daartoe bevoegde toezichthouder, of, de onder geheimhouding controlerende instantie in opdracht van Opdrachtgever toe te laten en verplicht medewerking te verlenen zodat de controle daadwerkelijk uitgevoerd kan worden.

7.3 Opdrachtgever zal controle slechts (laten) uitvoeren na een voorafgaande schriftelijke melding aan Wederpartij.

7.4 Wederpartij verbindt zich om binnen een door Opdrachtgever te bepalen termijn de Opdrachtgever, of de door Opdrachtgever ingeschakelde Derde, te voorzien van de verlangde informatie. Hierdoor kan de Opdrachtgever, of de door de Opdrachtgever ingeschakelde Derde, zich een oordeel vormen over de naleving door Wederpartij van deze verwerkersovereenkomst. De Opdrachtgever, of de door Opdrachtgever ingeschakelde Derde, is gehouden alle informatie betreffende deze controles vertrouwelijk te behandelen.

7.5 Wederpartij staat er voor in, de door Opdrachtgever of door Opdrachtgever ingeschakelde Derde, aangegeven aanbevelingen ter verbetering binnen de daartoe door de Opdrachtgever te bepalen redelijke termijn uit te voeren.

7.6 Wederpartij rapporteert jaarlijks over de opzet en werking van het stelsel van maatregelen en procedures, gericht op naleving van deze Verwerkersovereenkomst.

7.7 Naast rapportages door Wederpartij en controles door Opdrachtgever of controlerende instantie in opdracht van Opdrachtgever, kunnen beide Partijen ook overeenkomen gebruik te maken van een Third Party Memorandum (TPM) opgesteld door een onafhankelijke externe deskundige.

7.8 De redelijke kosten van de controle worden gedragen door de Partij die de kosten maakt, tenzij uit de controle blijkt dat Wederpartij enig punt uit deze Verwerkersovereenkomst niet heeft nageleefd. In dat geval worden de kosten van de controle gedragen door Wederpartij.

Artikel 8. Inschakeling derden

8.1 Wederpartij is slechts gerechtigd de uitvoering van werkzaamheden geheel of ten dele uit te besteden aan Derden na voorafgaande, duidelijk gespecificeerde of algemene, schriftelijke toestemming van Opdrachtgever.

8.2 Opdrachtgever kan aan de schriftelijke toestemming voorwaarden verbinden, op het gebied van geheimhouding en ter naleving van de verplichtingen uit deze Verwerkersovereenkomst.

8.3 Wederpartij blijft in deze gevallen te allen tijde aanspreekpunt en verantwoordelijk voor naleving van de bepalingen uit deze Verwerkersovereenkomst. Wederpartij garandeert dat deze Derden schriftelijk minimaal dezelfde plichten op zich nemen als tussen Opdrachtgever en Wederpartij zijn overeengekomen en zal Opdrachtgever, op diens verzoek, inzage verschaffen in de overeenkomsten met deze Derden waarin deze plichten zijn opgenomen.

8.4 Wederpartij garandeert dat iedere verwerking van Persoonsgegevens welke door of namens Wederpartij met inbegrip van de door hem ingeschakelde Derden wordt verricht in verband met het uitvoeren van de Overeenkomst binnen de Europese Economische Ruimte (EER) plaats zal vinden.

8.5 Wederpartij verschaft voorafgaand aan het sluiten van de Verwerkersovereenkomst inzicht in de locatie(s) waar de Verwerking plaatsvindt.

8.6 Het is 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.

8.7 Wederpartij houdt een actueel register bij van de door hem ingeschakelde Derden waarin de Identiteit, vestigingsplaats en een beschrijving van de werkzaamheden van de Derden zijn opgenomen, alsmede eventuele door de Opdrachtgever gestelde aanvullende voorwaarden.

Artikel 9. Wijziging en beëindigen verwerkersovereenkomst

9.1 Wijziging van deze Verwerkersovereenkomst kan slechts schriftelijk plaatsvinden middels een door beide Partijen geaccordeerd voorstel.

9.2 Bij beëindiging van de Overeenkomst, dan wel op eerste verzoek van Opdrachtgever gedurende de looptijd van de Overeenkomst, zal Wederpartij naar keuze van Opdrachtgever (i) alle of een door Opdrachtgever bepaald gedeelte van hem in het kader van deze Verwerkersovereenkomst ter beschikking gestelde Persoonsgegevens aan Opdrachtgever ter beschikking stellen (ii) alle of een door Opdrachtgever bepaald gedeelte van hem in het kader van deze Verwerkersovereenkomst ter beschikking gestelde Persoonsgegevens op alle locaties vernietigen, in welke vorm dan ook en toont dit aan, onverminderd de op hem rustende wettelijke verplichtingen. Opdrachtgever kan zo nodig nadere eisen stellen aan de wijze van beschikbaarstelling, waaronder eisen aan het bestandsformaat, dan wel vernietiging. Deze werkzaamheden moeten, binnen nader overeen te komen redelijke termijn, uitgevoerd worden en hiervan wordt een verslag gemaakt.

9.3 Wederpartij zal te allen tijde de in het vorige lid beschreven dataportabiliteit waarborgen zodanig dat er geen sprake is van verlies van functionaliteit of (delen van) de gegevens.

9.4 Opdrachtgever en Wederpartij treden met elkaar in overleg over wijzigingen in deze Verwerkersovereenkomst als een wijziging in de regelgeving of een wijziging in de uitleg van regelgeving daartoe aanleiding geven.

9.5 Indien Wederpartij tekort schiet in de nakoming van de verplichting op grond van deze Verwerkersovereenkomst kan Opdrachtgever hem in gebreke stellen waarbij Wederpartij alsnog een redelijke termijn voor nakoming wordt gegund. Blijft nakoming ook dan uit, dan is Wederpartij in verzuim. Ingebrekestelling is niet nodig wanneer voor de nakoming een fatale termijn geldt, nakoming blijvend onmogelijk is of indien uit een mededeling dan wel de houding van Wederpartij moet worden afgeleid dat deze in de nakoming van de verplichting op grond van deze Verwerkersovereenkomst zal tekort schieten.

9.6 Opdrachtgever is gerechtigd, onverminderd hetgeen daartoe bepaald is in de Verwerkersovereenkomst en de daarmee samenhangende Overeenkomst, en onverminderd hetgeen overigens in de wet is bepaald, de uitvoering van deze Verwerkersovereenkomst door middel van een aangetekend schrijven op te schorten, dan wel zonder rechterlijke tussenkomst met onmiddellijke ingang geheel of gedeeltelijk te ontbinden, nadat Opdrachtgever constateert dat:

a) Wederpartij (voorlopig) surseance van betaling aanvraagt; of
b) Wederpartij zijn faillissement aanvraagt of in staat van faillissement wordt verklaard; of
c) de onderneming van Wederpartij wordt ontbonden; of
d) Wederpartij zijn onderneming staakt; of

e) sprake is van een ingrijpende wijziging in de zeggenschap over de activiteiten van de onderneming van Wederpartij die maakt dat het in alle redelijkheid niet van Opdrachtgever kan worden verwacht dat hij de Verwerkersovereenkomst in stand houdt: of
f) op een aanmerkelijk deel van het vermogen van Wederpartij beslag wordt gelegd (anders dan door Opdrachtgever); of
g) Wederpartij aantoonbaar tekortschiet in de nakoming van de verplichtingen die voortvloeien uit deze Verwerkersovereenkomst en die toerekenbare tekortkoming niet binnen 30 dagen is hersteld na een daartoe strekkend schriftelijke ingebrekestelling dan wel een van de overige situaties bedoeld in artikel 9.5 zich voordoet.

Artikel 10. Aansprakelijkheid

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

10.2 Wederpartij is aansprakelijk op grond van artikel 82 van de Verordening voor alle schade of nadeel voortvloeiende uit het niet nakomen van, of in strijd handelen bij of krachtens de Verordening en/of de Uitvoeringswet 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.

10.3 Indien Wederpartij enig in de Verordening en/of de Uitvoeringswet genoemde verplichting niet nakomt, en er worden aan Opdrachtgever in verband hiermee (een) boetes opgelegd door de Autoriteit Persoonsgegevens dan wel een andere daartoe bevoegde toezichthouder, is Wederpartij een vergoeding verschuldigd aan Opdrachtgever, even groot als aan Opdrachtgever ter zake opgelegde boete, zonder dat hiervoor een aanmaning of een voorafgaande verklaring nodig is. Deze vergoeding is niet vatbaar voor verrekening en/of opschorting en laat het recht op nakoming en schadevergoeding onverlet. Tevens heeft opdrachtgever het recht om de Overeenkomst in bovengenoemde situatie met onmiddellijke ingang op te zeggen zonder dat Wederpartij aanspraak kan maken op enige vorm van schadevergoeding onverlet.

Artikel 11. Toepasselijk recht

11.1 Op deze Verwerkersovereenkomst en bijbehorende bijlagen en op alle geschillen die daaruit mogen voortvloeien of daarmee mogen samenhangen is uitsluitend het Nederlands recht van toepassing.

11.2 In geval van strijdigheid tussen het bepaalde in deze Verwerkersovereenkomst en het bepaalde in de Overeenkomst prevaleert het bepaalde in deze Verwerkersovereenkomst boven het bepaalde in de Overeenkomst.

Artikel 12. Overige bepalingen

12.1 Deze Verwerkersovereenkomst kan worden aangehaald als Verwerkersovereenkomst [naam].

Aldus in tweevoud opgesteld en getekend

Utrecht, [datum]	[plaats], [datum]
RUD Utrecht	[naam rechtspersoon]
Namens deze,	Namens deze,
.....	.....
H. Jungen	[naam]
directeur	[functie]

Bijlage 1: specificatie verwerking Persoonsgegevens

Deze bijlage specificeert de persoonsgegevens die namens Opdrachtgever door Wederpartij worden verwerkt, definieert het doel van deze verwerking en beschrijft de door Wederpartij getroffen beveiligingsmaatregelen.

Onderdeel I: doel van de verwerking
Opdrachtgever laat Persoonsgegevens door Wederpartij verwerken omdat Opdrachtgever gebruik wil maken van de Dienst [naam] van Wederpartij. Het doel van de verwerking heeft betrekking op [omschrijven].

Onderdeel II: categorieën betrokkenen
De Persoonsgegevens die in het kader van deze Verwerkersovereenkomst worden uitgewisseld hebben betrekking op de hieronder opgesomde betrokkenen:
Categorie 1: Medewerkers (dienstverband en inhuur) van de RUD Utrecht.
Categorie 2: Burgers van de volgende gemeenten:
Categorie 3: Medewerkers van de volgende gemeenten:
Categorie 4: Contactpersonen bij de volgende bedrijven:

Onderdeel III: de te verwerken persoonsgegevens
De onderstaande tabel toont de Persoonsgegevens die Wederpartij namens Opdrachtgever Verwerkt. Het gaat niet enkel om Persoonsgegevens die Opdrachtgever direct aan Wederpartij verstrekt, maar ook om Persoonsgegevens die Gebruiker aanlevert bij gebruik van de Dienst.

Categorie Betrokkene	Persoonsgegevens
Nummers invullen	Opsomming per regel

Onderdeel IV: getroffen beveligingsmaatregelen
De door Wederpartij getroffen beveiligingsmaatregelen betreffen in ieder geval de maatregelen die zijn beschreven in de bijgevoegde en door Wederpartij ondertekende Bijlage 2 "Richtlijn beveiligingsafspraken derden".

Indien van toepassing wordt ook door Wederpartij aan Opdrachtgever ter hand gestelde beveiligingsdocumentatie of (audit / assurance) rapporten toegevoegd aan deze

Verwerkersovereenkomst voor zover deze geen onderdeel zijn van de Overeenkomst zoals bedoeld in artikel 1.5.

Onderdeel V: Informatie die moet worden verstrekt bij een datalek

Als Wederpartij Opdrachtgever moet informeren op grond van artikel 6 van de Verwerkersovereenkomst, moet hij de volgende gegevens 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 voorgedaan.
- Verstrekt – voor zover mogelijk – de gegevens zoals opgenomen in artikel 33 lid 3 van de Verordening.

Vervolgacties naar aanleiding van het Datalek

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

Paraaf RUD Utrecht	Paraaf [naam rechtspersoon]
…….	……
H. Jungen	[naam]
directeur	[functie]

BIJLAGE 2.

RICHTLIJN BEVEILIGINGSAFSPRAKEN DERDEN

Inhoudsopgave

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 RUD Utrecht 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 RUD Utrecht dat er goede afspraken worden gemaakt op het gebied van informatiebeveiliging. Dit voorkomt niet alleen onnodige discussies in de praktijk, maar maakt ook aantoonbaar dat de RUD Utrecht haar wettelijke verantwoordelijkheid neemt. De wet stelt namelijk dat de RUD Utrecht ook verantwoordelijk is voor de beveiliging van haar informatie bij leveranciers en partners. Werkzaamheden kunnen worden uitbesteed, maar verantwoordelijkheden niet.

1.1 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 Information Security Officer heeft 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 Information Security Officer voorafgaand aan ondertekening verwerkt in een hoofdstuk 3 van deze richtlijn. Vervolgens wordt voorliggend document inclusief een eventuele bijlage met afwijkingen, toegevoegd als bijlage bij een overeenkomst met een leverancier.

Wanneer de Information Security Officer constateert dat de informatiebeveiliging van de leverancier onvoldoende is, dan wordt het aangaan van een overeenkomst uitgesteld tot het moment dat de leverancier wèl aan beveiligingseisen van de RUD Utrecht voldoet.

1.2 Definities

Met "(interne) gebruikers/beheerders" worden niet alleen gebruikers/beheerders van de RUD Utrecht bedoeld (intern), maar ook gebruikers/beheerders aan de leveranciers zijde.

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

2 Uitgangspunten

2.1 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	De netwerkverbinding tussen relaties (klanten/partners) en de (web)applicatie is adequaat versleuteld[1] indien er vertrouwelijke gegevens worden uitgewisseld.
	Gezien het openbare karakter van internet dienen vertrouwelijke gegevens, zoals bijvoorbeeld persoonsgegevens, 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.

2.2 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 RUD Utrecht[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 RUD Utrecht (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 RUD Utrecht[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 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.

[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.

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 RUD Utrecht. Bijvoorbeeld wanneer deze toegang hebben tot het LAN van de RUD Utrecht. 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 RUD Utrecht[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 RUD Utrecht.
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 RUD Utrecht 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. Backups 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.
	Met het beperken van toegang tot vertrouwelijke data wordt misbruik van deze data voorkomen.

2.3 Patchmanagement

ID	Uitgangspunt

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

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, zijn 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.

2.4 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 RUD Utrecht 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 RUD Utrecht of de inhoud van de aan de RUD Utrecht toegekende database(tabellen).
	Alleen gebruikers en beheerders van de RUD Utrecht dienen de mogelijkheid te hebben data van de RUD Utrecht 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.

2.5 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.

2.6 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.

[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

2.7 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 RUD Utrecht conform een beveiligingsmanagementsysteem (ISMS) waarin minimaal de relevante onderdelen uit de ISO 27002 zijn opgenomen.
	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.

2.8 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.
	Monitoring helpt om problemen te signaleren en tijdig met een oplossing te kunnen komen zodat de beschikbaarheidsgaranties kunnen worden waargemaakt.

2.9 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 RUD Utrecht, 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 VOG[6] aan te vragen.
	De systeemrechten die aan beheerpersoneel zijn toegekend geven toegang tot (vertrouwelijke) data van de RUD Utrecht. De kans op fraude door personeel dient te worden beperkt.
RBD31	Beheerpersoneel (of ander personeel met toegang tot gegevens van de RUD Utrecht) heeft een verklaring ondertekent die de geheimhouding van gegevens van de RUD Utrecht 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 RUD Utrecht te voorkomen.

2.10 **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 RUD Utrecht 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 RUD Utrecht[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

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

	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.

2.11 **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 mogelijk wordt in plaats van met detailgegevens, gewerkt met een relatienummer dat door de RUD Utrecht 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 bewerkersovereenkomst 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 bewerkersovereenkomst met derden is een verplichting die voortkomt uit de Wet bescherming persoonsgegevens (Wbp) en de Algemene Verordening Gegevensbescherming (AVG). Het helpt de RUD Utrecht om controle te houden over de wijze waarop een derde partij met door de RUD Utrecht vergaarde persoonsgegevens omgaat. Het opstellen van een bewerkersovereenkomst 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 RUD Utrecht.
	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 Wbp vastgelegde uitzonderingen, niet toegestaan.

2.12 **Clouddiensten**

ID	Uitgangspunt
RBD44	Wanneer de leverancier de gegevens van de RUD Utrecht 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 RUD Utrecht.
	Om te borgen dat (persoons)gegevens van de RUD Utrecht volledig conform de Nederlandse wet (en het daarop gebaseerde beleid van de RUD Utrecht) worden behandeld, zijn buitenlandse cloudvoorzieningen mogelijk ongeschikt. Uitwisseling vanuit Nederland naar andere EU-lidstaten is mogelijk op basis van de Nederlandse Wbp. 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 bewerkersovereenkomst verplicht.

2.13 **Toetsing**

ID	Uitgangspunt
RBD45	Aan het eind van het traject/project kan de RUD Utrecht besluiten een penetratietest uit te (laten) voeren met deze richtlijn als (minimale) norm. Daarnaast worden nieuwe releases en major updates (upgrades) door de RUD Utrecht 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 RUD Utrecht of een door de RUD Utrecht 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).
	Hiermee wordt voorkomen dat de RUD Utrecht (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 RUD Utrecht afloopt.

3 Overeengekomen afwijkingen

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

ID	Beschrijven van de afwijking

4 Ondertekening

Door ondertekening van deze overeenkomst verklaart de leveranciers van de RUD Utrecht zich te conformeren aan de uitgangspunten beschreven in hoofdstuk 2 van deze richtlijn met in acht neming van de geformuleerde afwijkingen in hoofdstuk 3.

Als onderdeel van de ondertekening dient ook iedere pagina te worden voorzien van een paraaf van de ondertekenaar.

Naam _____

Functie _____

Organisatie _____

Datum _____

Handtekening _____