PRIVACYBELEID

Versie	0.4
Datum	februari 2018
Auteur	ir. Dennis Baaten CISSP
Classificatie	Intern

Inhoudsopgave

1 Documenthistorie en goedkeuring

1.1 Documenthistorie

Versie	Datum	Gewijzigd door	Aard van de wijziging
0.1	31-10-2017	Dennis Baaten	Eerste opzet
0.2	24-01-2018	Dennis Baaten	Diverse verbeteringen. • Toevoegen doelbinding bij eisen overeenkomst. • Verwerken van impact concept wetsvoorstel Uitvoeringswet AVG op “bijzondere persoonsgegevens”. • Aanscherpen onderdelen: rechten betrokkenen, encryptie, verwerker, privacy by design en privacy by default, DPIA. • Toevoegen toelichting op gebruik testdata. • Separaat hoofdstuk functionaris gegevensbescherming.
0.3	01-02-2018	Dennis Baaten	Aanpassingen/toevoegen in hoofdstuk 9.1 en 9.2 inzake het vaststellen van verwerkerschap.
0.4	08-02-2018	Dennis Baaten	Aanscherpen boetes in hoofdstuk 13.

1.2 Goedkeuring

Voorliggend document is een onderdeel van het informatiebeveiligingsbeleid van de Regionale Uitvoeringsdienst (RUD) Utrecht en is goedgekeurd door de directie.

Hugo Jungen
Directeur

Handtekening: _____ Datum: _____

2 Inleiding

Dit document beschrijft het privacybeleid van de Regionale Uitvoeringdienst (RUD) Utrecht gebaseerd op de Algemene Verordening Gegevensbescherming (AVG). Deze verordening vervangt de oude Nederlandse Wet bescherming persoonsgegevens (Wbp), is op 25 mei 2016 in werking getreden, en wordt vanaf 25 mei 2018 van kracht en gehandhaafd door de Nederlandse toezichthouder: de Autoriteit Persoonsgegevens (AP). Organisaties die niet voldoen aan de wet riskeren hoge boetes.

De AVG laat ruimte aan lidstaten om een (strenger) beleid ten aanzien van privacy te voeren. Binnen Nederland gebeurt dit met de nationale wet Uitvoeringswet AVG (UAVG). Deze nationale wet geeft invulling aan elementen waarover de Europese lidstaten geen consensus konden bereiken in de AVG, en aan zaken die op Europees niveau niet zijn benoemd. Denk bijvoorbeeld aan het BSN-nummer dat binnen Nederland wordt gezien als een identificatienummer dat een bijzondere bescherming toekomt.

Daarnaast is het belangrijk om te beseffen dat er nog geen jurisprudentie bestaat ten aanzien van onderwerpen in de AVG. Gedurende de komende jaren zullen rechters dus gaan bepalen hoe bepaalde zaken het beste geïnterpreteerd en geïmplementeerd kunnen worden. Het beschikbaar komen van jurisprudentie kan wijzigingen in dit beleidsdocument tot gevolg hebben.

3 Definities en begrippen

In dit document, maar ook in verschillende wetteksten worden specifieke termen en begrippen gebruikt. In dit hoofdstuk worden deze toegelicht.

AVG – de Europese privacywet ‘Algemene Verordening Gegevensbescherming’ (AVG) is sinds 25 mei 2018 van kracht voor alle lidstaten van de Europese Unie. Deze wet wordt in het Engels ook wel General Data Protection Regulation (GDPR) genoemd.

Uitvoeringswet AVG – dit is de Nederlandse nationale wet waarin Nederland invulling geeft aan zaken die op Europees niveau niet zijn benoemd in de AVG.

Verwerkingsverantwoordelijke – een verwerkingsverantwoordelijke is verantwoordelijk voor de verwerking(en) van persoonsgegevens, ook wanneer er sprake is van verwerking door derden. De verwerkingsverantwoordelijke bepaalt zelf het doel van en de middelen voor de verwerking.

Verwerker – een verwerker verwerkt persoonsgegevens in opdracht van of ten behoeve van een verwerkingsverantwoordelijke.

Verwerkersovereenkomst – Wanneer verwerking van persoonsgegevens wordt uitbesteed of wanneer er persoonsgegevens van een andere partij worden verwerkt, moeten er afspraken worden gemaakt tussen de verwerkingsverantwoordelijke en de verwerker. Deze afspraken dienen te worden vastgelegd in een zogenaamde verwerkersovereenkomst.

Verwerkingsregister – Dit is een vanuit de AVG verplicht register wat door organisaties wordt bijgehouden en waarin is vastgelegd wat voor persoonsgegevens zij opslaan of verwerken, van wie deze persoonsgegevens zijn, waar dit wordt opgeslagen en hoe dit is beveiligd.

Betrokkene – dit betreft de persoon of personen wiens gegevens worden verwerkt. Bijvoorbeeld klanten, partners of medewerkers.

Persoonsgegevens – dit betreft alle informatie waarmee een natuurlijk persoon direct of indirect kan worden geïdentificeerd. Gegevens waarmee direct kan worden geïdentificeerd zijn identificatoren zoals een naam, identificatienummer en locatiegegevens. Gegevens die mede bepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld, en ook gegevens die in combinatie met andere gegevens leiden tot identificeerbaarheid, dienen ook te worden beschouwd als persoonsgegevens. Voorbeelden zijn gegevens over: inkomen, vermogen, beroep, woonplaats en leeftijd.

Bijzondere persoonsgegevens – zijn naar hun aard vertrouwelijker dan 'gewone' persoonsgegevens en verwerking ervan geschiedt op andere gronden dan 'gewone' persoonsgegevens. Het vertrekpunt is dat verwerking van deze categorieën van gegevens verboden is, tenzij aan een aantal voorwaarden is voldaan zoals genoemd in de AVG of de uitvoeringswet.

4 Verwerkingsbeginselen

De AVG introduceert kernbeginselen waaraan alle verwerkingen van persoonsgegevens moeten voldoen. De verwerkingsverantwoordelijke moet kunnen bewijzen dat wordt voldaan aan deze verwerkingsbeginselen. De verantwoordelijke kan hier natuurlijk afspraken over maken met de verwerker.

Doelbinding – persoonsgegevens mogen alleen voor een bepaald, uitdrukkelijk omschreven doel worden verwerkt. Dit dient te worden vastgelegd in een overeenkomst tussen verwerkingsverantwoordelijke en verwerker. De persoonsgegevens mogen dus niet voor andere doeleinden worden gebruikt, en het doel kan nooit eenzijdig worden aangepast.

Rechtmatigheid – persoonsgegevens mogen alleen worden verwerkt wanneer aan de tenminste één van de volgende grondslagen is voldaan (wanneer er een grondslag is voor de verwerking):

- er is toestemming van de betrokkene;
- de verwerking is noodzakelijk voor de uitvoering van een overeenkomst;
- de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting;
- de verwerking is noodzakelijk om de vitale belangen van betrokkene of andere natuurlijke personen te beschermen;
- de verwerking is noodzakelijk ter vervulling van een taak van algemeen belang of openbaar gezag;
- de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde.

Dataminimalisatie – uitsluitend voor het doel noodzakelijke gegevens mogen worden verwerkt, en niet meer dan dat.

Datakwaliteit – de verwerkingsverantwoordelijke heeft een vergaande verplichting om te borgen dat gegevens compleet, juist en bruikbaar zijn. Dit hangt deels samen met de verplichting om persoonsgegevens te beveiligingen door het nemen van voldoende technische en organisatorische maatregelen.

Verwerkingsduur – gegevens mogen worden verwerkt gedurende een specifieke vastgestelde periode, en ze mogen voor slechts bepaalde tijd worden bewaard. De organisatie stuurt hier actief op.

Transparantie – de verwerkingsverantwoordelijke zorgt dat verwerking van persoonsgegevens transparant plaatsvindt, en kan zodoende rekenschap afleggen over de exacte verwerking van de persoonsgegevens.

Verantwoordingsplicht – de verwerkingsverantwoordelijke moet verantwoording kunnen afleggen aan de toezichthouder en de betrokkenen. Verwerkingsverantwoordelijke moet hiertoe rekenschap kunnen afleggen over de aard en het doel van de verwerking.

De verwerkingsverantwoordelijke moet kunnen bewijzen dat wordt voldaan aan deze verwerkingsbeginselen. De verantwoordelijke kan hier natuurlijk afspraken over maken met de verwerker.

De AVG stelt dat de verwerking van persoonsgegeven met een duidelijk doel verbonden en context gebonden dient te zijn. In de praktijk betekent dit dat persoonsgegevens alleen verwerkt mogen worden als er een legitieme doelstelling achter ligt. Overmatige verwerking van persoonsgegevens is niet toegestaan. Bovendien mogen de gegevens niet zonder toestemming gebruikt worden voor de levering van andere producten of diensten.

➔ *Doel en context van de verwerking worden binnen de RUD Utrecht enerzijds vastgelegd in een verwerkingsregister en anderzijds in overeenkomsten met verwerkers (dit komt nog aan bod in hoofdstuk 9). Let op: ook de eigen verwerkingen dienen te worden vastgelegd in het verwerkingsregister.*

➔ *In het verwerkingsregister wordt, indien van toepassing, ook bijgehouden of er toestemming is gegeven door de betrokkenen om de gegevens te mogen verwerken.*

5 Persoonsgegevens en bijzondere persoonsgegevens

5.1 Persoonsgegevens

Persoonsgegevens betreft alle informatie waarmee een natuurlijk persoon direct of indirect kan worden geïdentificeerd. Gegevens waarmee direct kan worden geïdentificeerd zijn identificatoren zoals een naam, identificatienummer en locatiegegevens.

Gegevens die mede bepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld, en ook gegevens die in combinatie met andere gegevens leiden tot identificeerbaarheid, dienen ook te worden beschouwd als persoonsgegevens. Voorbeelden zijn gegevens over: inkomen, vermogen, beroep, woonplaats en leeftijd.

De AVG verruimt de definitie van het begrip persoonsgegevens. Voor de beeldvorming hieronder een aantal voorbeelden van informatie die worden gezien als persoonsgegevens:

- Voornaam en achternaam
- Adres
- BSN
- Identificatienummers
    - Personeelsnummer
    - Klantnummer
    - Patiëntnummer
    - Bankrekeningnummer
- Geboortedatum / leeftijd
- Locatiegegevens
- Online identificatoren
    - IP-adres
    - MAC-adres
    - Cookies (ook als de naam van de persoon achter het cookie niet bekend is)
    - RFID tag
    - IMEI nummer
- E-mailadres
- Vingerafdruk
- Pasfoto
- Iemands IQ
- Gebruikersnaam
- Persoonskenmerken zoals gewicht, lengte, haarkleur en geslacht

5.2 Bijzondere persoonsgegevens

Het verwerken van bijzondere persoonsgegevens is verboden, tenzij er aan de voorwaarden van de AVG óf aan de uitzonderingen zoals genoemd in de Uitvoeringswet AVG wordt voldaan.

De volgende gegevens worden gezien als bijzondere persoonsgegevens (artikel 9 lid 1):
- Ras of etnische afkomst;
- Politieke opvattingen;
- Religieuze of levensbeschouwelijke overtuigingen;

- Lidmaatschap van een vakbond;
- Genetische gegevens;
- Biometrische gegevens met het oog op de unieke identificatie van een persoon;
- Gegevens over gezondheid;
- Seksueel gedrag of seksuele gerichtheid;
- Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten (artikel 10 AVG, artikel 32 en 33 UAVG).

In het memorie van toelichting op het wetsvoorstel van de UAVG staat dat indirecte informatie ook als bijzondere persoonsgegevens worden gezien:

> "Een persoonsgegeven is niet alleen bijzonder wanneer het direct het desbetreffende bijzondere onderwerp onthult. Ook gegevens die indirect dergelijke informatie onthullen, worden aangemerkt als bijzondere categorieën van persoonsgegevens. Tot de bijzondere categorieën van persoonsgegevens moeten dus niet alleen gegevens worden gerekend die direct betrekking hebben op bijvoorbeeld het lidmaatschap van een vakbond als zodanig, maar ook gegevens waaruit iemands vakbondslidmaatschap indirect valt af te leiden. De administratie van een vakbond, met daarin namen en adressen van de leden, is daarvan een voorbeeld. Noodzakelijk is wel dat er een rechtstreeks verband is. Gegevens die hooguit een indicatie geven dat het om een gevoelig kenmerk zou kunnen gaan, vallen buiten de reikwijdte van de bijzondere regeling voor gevoelige gegevens."

De AVG noemt in artikel 9 lid 2 de volgende voorwaarden voor verwerking van bijzondere persoonsgegevens:

- De betrokkene heeft uitdrukkelijk toestemming gegeven voor de verweking, tenzij is bepaald dat het verbod niet door de betrokkene kan worden opgeheven;
- De verwerking is noodzakelijk om wettelijke plichten of rechten te dienen binnen het arbeidsrecht of socialezekerheids- en socialebeschermingsrecht;
- Wanneer de verwerking van vitaal belang (levensbelang) is voor de betrokkene, en deze niet in staat is om zelf toestemming te geven;
- Verwerking vindt plaats door politieke, religieuze, levensbeschouwelijke organisaties of vakbonden, waarbij de verwerking noodzakelijk is voor het onderhouden van contact met leden of voormalige leden;
- De verwerking heeft betrekking op gegevens die de door de betrokkene zelf openbaar zijn gemaakt;
- Wanneer de verwerking noodzakelijk is in het kader van gerechtelijke procedures;
- Wanneer de verwerking noodzakelijk is voor een zwaarwegend algemeen belang dat bij wet is vastgelegd;
- Wanneer de verwerking noodzakelijk is voor medische redenen, met name in verband met de arbeid (het medisch beroepsgeheim blijft van toepassing);
- Wanneer de verwerking nodig is in het algemeen belang op het gebied van de volksgezondheid;
- Wanneer de verwerking noodzakelijk is voor archivering in het openbaar belang of voor onderzoek of statistiek.

Daarnaast benoemd de UAVG in artikel 22 tot en met artikel 33 ook een aantal uitzonderingen die van toepassing zijn op de verwerking van bijzondere persoonsgegevens. Deze uitzonderingen komen grotendeels overeen met de uitzonderingen die in de AVG worden genoemd, maar in een aantal gevallen wijkt de uitzondering af. In dergelijke gevallen is in Nederland de UAVG leidend. De meest opvallende afwijkingen zijn:

- In de UAVG wordt het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken, niet van toepassing verklaard indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden. Het verwerken voor biometrische gegevens is dus toegestaan zolang dit voor authenticatie of beveiligingsdoeleinden gebeurt.

➔ *Medewerkers van de RUD Utrecht dienen bewust te worden gemaakt van de soorten persoonsgegevens die er zijn, en welke door RUD Utrecht worden verwerkt. Tijdens een*

bewustwordingscampagne AVG is er ook aandacht voor de impact van de AVG op bestaande processen, procedures en werkwijzen.

➔ *De RUD Utrecht legt de voor medewerkers geldende omgangsvormen vast in een gedragscode.*

6 Rechten betrokkenen

De rechten van betrokkenen ten aanzien van de verwerkingsverantwoordelijke zijn onder de AVG aanzienlijk versterkt. Om de juiste naleving van de AVG zelfstandig en/of makkelijker af te kunnen dwingen (de zogenaamde horizontale handhaving) heeft de betrokkene hiertoe de volgende rechten en middelen:

- Recht op informatie;
- Recht van inzage;
- Recht op rectificatie;
- Recht op gegevenswissing/vergetelheid;
- Recht op beperking van de verwerking;
- Recht op overdraagbaarheid/dataportabiliteit;
- Recht van bezwaar;
- Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming/profilering.

Organisaties die optreden als verwerkingsverantwoordelijke dienen te borgen dat betrokkenen zich te allen tijde kosteloos kunnen beroepen op deze rechten, en dat er binnen de wettelijk geldende termijn van één maand dient te worden gereageerd op verzoeken van betrokkenen. Een verlenging met maximaal twee maanden is mogelijk, mits die binnen één maand wordt gemeld en de extra benodigde tijd goed is onderbouwd.

Organisaties die optreden als verwerker van persoonsgegevens kunnen verzoeken van betrokkenen met betrekking tot de persoonsgegevens die ze verwerken in opdracht van verwerkingsverantwoordelijke, afwijzen. Wel kan het zo zijn dat de verwerkingsverantwoordelijke aan verwerker vraagt om bepaalde gegevens op te leveren. Vanuit de AVG is de verwerker verplicht om aan dergelijke verzoeken mee te werken.

Inzichtelijkheid en het recht om vergeten te worden. Natuurlijke personen hebben volgens de AVG het recht om in te zien welke gegevens van hen elektronisch door verwerkingsverantwoordelijke zijn vastgelegd en hieruit verwijderd te worden. Voor organisaties betekent dit niet alleen middels een veilige wijze deze gegevens moeten delen, ook betekent dit dat van organisaties hun informatiehuishouding rondom persoonsgegevens duidelijk en bekend moet zijn.

➔ *De RUD Utrecht dient tijdig aan rechten van betrokkenen gehoor te kunnen geven. Ook kunnen klanten van de RUD Utrecht (die diensten leveren aan consumenten) namens consumenten zich beroepen op deze rechten. Hiervoor kan bijvoorbeeld worden gedacht aan:*
  - *Een procedure voor het verwijderen van gegevens;*
  - *Een procedure voor het verlenen van inzage in gegevens;*
  - *Een procedure voor het overdragen van gegevens;*
  - *Een procedure voor het muteren van gegevens.*

➔ *De RUD Utrecht publiceert een privacybeleid op de website waarin staat beschreven tot wie personen zich kunnen wenden voor vragen.*

➔ *Verzoeken van betrokkenen die van toepassing zijn op persoonsgegevens die door de RUD Utrecht verwerkt worden in de rol van verwerker, worden afgewezen door betrokkenen mede te delen dat de RUD Utrecht die informatie vanuit haar rol als verwerker niet mag verstrekken, en dat ze zich hiervoor kunnen wenden tot de verwerkingsverantwoordelijke.*

7 Datalekken

De wet spreekt van een datalek wanneer persoonsgegevens verloren raken of onrechtmatige verwerking redelijkerwijs niet kan worden uitgesloten. Wanneer dit het geval is dient het datalek binnen 72 uur te worden gemeld aan de Autoriteit Persoonsgegevens, en mogelijk ook aan de betrokkenen. Hiervoor kan het richtsnoer meldplicht datalekken[1] van de Autoriteit Persoonsgegevens worden geraadpleegd.

De definitie van onrechtmatige verwerking is breed. Het betreft onder andere het aanpassen en/of veranderen van persoonsgegeven en onbevoegde toegang tot, of afgifte daarvan. Er is dus niet alleen sprake van een datalek als een hacker toegang tot persoonsgegevens krijgt. Er is bijvoorbeeld ook sprake van een datalek in de volgende situaties:

- Verlies van een USB-stick in de trein.
- Het sturen van een mailing met adressen in het AAN of CC veld (in plaats van het BCC veld).
- Het verliezen van gegevens als gevolg van een brand in het datacentrum terwijl er geen backup beschikbaar is.
- De onbevoegde ongedaanmaking van pseudonimisering (hoofdstuk 8.3) en/of encryptie (hoofdstuk 8.4).

Er is een procedure voor het melden van datalekken wanneer onrechtmatige verwerking niet kan worden uitgesloten (artikel 33 en 34).

➔ *De RUD Utrecht beschikt over een procedure voor het melden van datalekken.*

➔ *De RUD Utrecht beschikt over middelen om vast te stellen of er sprake is van datalekken. Denk bijvoorbeeld aan logging en monitoring.*

7.1 Inbreukenregister

De AVG verplicht verwerkingsverantwoordelijke tot het documenteren van alle inbreuken in verband met persoonsgegevens, inclusief de gevolgen en de genomen maatregelen om dit in de toekomst te voorkomen (artikel 33 lid 5). Ook wanneer deze inbreuken nadrukkelijk niet hebben geleid tot een datalek. De Autoriteit Persoonsgegevens kan toegang verlangen tot deze documentatie (artikel 58 lid 1 punt a), en de documentatie moet adequaat zijn om de toezichthouder te laten controleren of datalekken daadwerkelijk worde gemonitord en opgevolgd.

Onder ‘inbreuk in verband met persoonsgegevens’ wordt verstaan; wanneer persoonsgegevens zijn vernietigd of verloren, gewijzigd, verstrekt of toegankelijk zijn gemaakt. Zie ook artikel 4 lid 12 voor de definitie in de AVG.

Voor organisaties in de rol van verwerker betekent dit eveneens dat zij een inbreukenregister dienen bij te houden. Verwerkingsverantwoordelijken kunnen er namelijk om vragen.

➔ *De RUD Utrecht beschikt over een inbreukenregister waarin alle inbreuken in relatie tot persoonsgegevens volgens de eisen van de AVG worden vastgelegd.*

8 Technische en organisatorische maatregelen

Verwerkingsverantwoordelijke en verwerker moeten passende technische en organisatie maatregelen nemen om zogenaamde onrechtmatige verwerkingen van persoonsgegevens te voorkomen. De term ‘passend’ kan worden bepaald door te kijken naar het risico in verhouding tot de mogelijkheden en kosten om het risico af te dekken.

Er worden passende technische en organisatorische maatregelen genomen om te voorkomen dat persoonsgegevens onrechtmatige worden verwerkt (artikel 32);

[1] Het richtsnoer is hier te vinden: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

➔ *De RUD Utrecht heeft een informatiebeveiligingsbeleid van waaruit passende beveiligingsmaatregelen worden opgelegd en wordt geborgd dat deze geïmplementeerd zijn en blijven.*

Met de richtlijn beveiligingsafspraken derden wordt geborgd dat leveranciers voldoende maatregelen nemen om persoonsgegevens te beschermen. Aangezien de RUD Utrecht geen eigen ICT voorzieningen onderhoudt, kan met deze richtlijn grotendeels invulling worden gegeven aan de wettelijke eis van een 'passend beveiligingsniveau'.

Een aantal maatregelen worden expliciet benoemd in de AVG. Deze maatregelen worden in de volgende paragrafen nader toegelicht.

8.1 Data protection impact assessment (DPIA)

De AVG verplicht organisaties tot het uitvoeren van een DPIA (in het Nederlands de gegevensbeschermingseffectbeoordeling) wanneer er wijzigingen in de verwerking van persoonsgegevens worden doorgevoerd die mogelijk/waarschijnlijk een hoog risico (een potentiële inbreuk) inhouden voor de rechten en vrijheden van natuurlijke personen (betrokkenen). Zie ook de definitie in artikel 35, lid 1. De achterliggende gedachte is dat de DPIA inzicht geeft in de risico's waardoor de juiste maatregelen genomen kunnen worden om de risico's tot een acceptabel niveau te verlagen.

Artikel 35, lid 3 uit de AVG geeft enkele voorbeelden van wanneer een verwerking "waarschijnlijk een hoog risico inhoudt":

a. Geautomatiseerde beoordeling van personen - een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen.
b. Grootschalige verwerking van bijzondere persoonsgegevens - grootschalige verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9, lid 1, of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10.
c. Grootschalig monitoren van openbare ruimtes - stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

De 'werkgroep artikel 29' (WP29) probeert dit verder te concretiseren, en noemt negen criteria die in aanmerking moeten worden genomen bij het beoordelen of een verwerking een "waarschijnlijk hoog risico" inhoudt. WP29 geeft aan dat het voldoen aan twee van de negen criteria vaak al betekent dat een DPIA dient te worden uitgevoerd.

1. Evaluatie of scoretoekenning – onder andere profielbepalingen en voorspelling in het kader van kenmerken betreffende beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen van de betrokkene.
2. Geautomatiseerde besluitvorming met rechtgevolg of vergelijkbaar wezenlijk gevolg – verwerkingen die gericht zijn op het nemen van beslissingen met betrekking tot betrokkenen "waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden" of die "de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen".
3. Stelselmatige monitoring - verwerkingen die worden gebruikt voor het observeren, monitoren of controleren van betrokkenen, inclusief via netwerken verzamelde gegevens of stelselmatige monitoring van openbaar toegankelijke ruimten.
4. Gevoelige gegevens of gegevens van zeer persoonlijke aard (bijzondere persoonsgegevens) - dit omvat speciale categorieën persoonsgegevens zoals omschreven in artikel 9 (bijvoorbeeld informatie over de politieke opvattingen van personen), evenals persoonsgegevens met betrekking tot strafrechtelijke veroordelingen of strafbare feiten zoals omschreven in artikel 10.
5. Op grote schaal verwerkte gegevens

6. Matching of samenvoeging van datasets – bijvoorbeeld datasets die voortkomen uit twee of meer gegevensverwerkingen die voor verschillende doeleinden zijn uitgevoerd en/of door verschillende verwerkingsverantwoordelijken zijn uitgevoerd op een wijze die de redelijke verwachtingen van de betrokkene zou overschrijden.
7. Gegevens met betrekking tot kwetsbare betrokkenen – verwerkingen van dit soort gegevens is een criterium vanwege de toegenomen machtsongelijkheid tussen de betrokkenen en de verwerkingsverantwoordelijke, wat betekent dat de natuurlijke personen mogelijk niet in staat zijn om gemakkelijk in te stemmen met of bezwaar te maken tegen de verwerking van hun gegevens, of om hun rechten uit te oefenen. Kwetsbare betrokkenen kunnen kinderen omvatten, werknemers, kwetsbaardere segmenten van de bevolking die speciale bescherming behoeven (bijvoorbeeld geesteszieken, asielzoekers, bejaarden, patiënten), maar ook ander situaties waarin een onevenwichtigheid in de relatie tussen de positie van de betrokkene en de verwerkingsverantwoordelijke kan worden vastgesteld.
8. Innovatief gebruik of innovatieve toepassing van nieuwe technologische of organisatorische oplossingen – bijvoorbeeld het combineren van het gebruik van vingerafdrukken en gezichtsherkenning voor een betere fysieke toegangscontrole. In de AVG wordt duidelijk gesteld (artikel 35, lid 1) dat het gebruik van een nieuwe technologie aanleiding kan geven tot de noodzaak om een DPIA uit te voeren. Dit komt omdat het gebruik van dergelijke technologie nieuwe vormen van het verzamelen en gebruiken van gegevens kan inhouden, mogelijk met een hoog risico voor de rechten en vrijheden van natuurlijke personen. De persoonlijke en sociale gevolgen van het gebruik van een nieuwe technologie kunnen immers onbekend zijn.
9. Wanneer als gevolg van de verwerking zelf betrokkenen een recht niet kunnen uitoefenen of geen beroep kunnen doen op een dienst of een overeenkomst (artikel 22) – bijvoorbeeld verwerkingen die erop gericht zijn de toegang van betrokkenen tot een dienst of de mogelijkheid van betrokkenen om een overeenkomst aan te gaan, toe te staan, te wijzigen of te weigeren.

Het toepassen van een DPIA werk in feite als een drietrapsraket:
1. Bij iedere verwerking moet de verwerkingsverantwoordelijke een eerste beoordeling maken van de risico's die daarbij kunnen bestaan (classificatie);
2. Wanneer uit de eerste beoordeling blijkt dat er sprake is van een hoog risico, dan dient een uitgebreide DPIA worden uitgevoerd;
3. Wanneer uit de DPIA blijkt dat het hoge risico niet kan worden beperkt met redelijke middelen, dan moet de toezichthouder eerst worden geraadpleegd.

Organisaties zijn verplicht tot het uitvoeren van een 8.1 Data Protection Impact Assessment (DPIA) wanneer er iets wijzigt in de verwerking van persoonsgegevens, of wanneer zij van plan zijn om persoonsgegevens te gaan verwerken en dit waarschijnlijk een hoog risico voor de betrokkene inhoudt (artikel 35).

Let op: de Autoriteit Persoonsgegevens heeft aangekondigd dat zij binnenkort een lijst publiceert met type wijzigingen die een DPIA vereisen (conform artikel 35 lid 4). Zodra deze lijst beschikbaar is, zal deze worden opgenomen in dit beleidsdocument. Hiermee wordt getracht iets duidelijker te maken voor welke type wijzigingen een DPIA is vereist.

➔ *De RUD Utrecht legt de criteria voor het uitvoeren van een DPIA classificatie (de eerste stap in het drietrapsmodel) vast, zodat deze binnen de organisatie toegepast kunnen worden. Hiervoor wordt de lijst gebruikt die door de Autoriteit Persoonsgegevens wordt gepubliceerd.*

➔ *De RUD Utrecht is verplicht tot het uitvoeren van een DPIA classificatie en (afhankelijk van de uitkomst) ook een uitgebreide DPIA, alvorens het verstrekken van opdrachten aan leveranciers tot wijzigingen in de ICT omgeving die van invloed zijn op de wijze waarop persoonsgegeven worden verwerkt.*

8.2 Privacy by design

De AVG verplicht verwerkingsverantwoordelijken om invulling te geven aan de begrippen *privacy by design* en *privacy by default*. Dit betekent echter niet dat verwerkers er niks mee te maken hebben. Ook deze zullen een invulling moeten geven aan deze begrippen. Al is het maar omdat klanten

(verwerkingsverantwoordelijken) hierom (gaan) vragen. Daarnaast is het doorgaans veel duurder om *privacy by design* met terugwerkende kracht door te voeren (bolt-on) dan hier bij het ontwikkelproces al rekening mee te houden (build-in).

Dit betekent dat de ICT voorzieningen die de RUD Utrecht inzet voor haar bedrijfsvoering zodanig dient te zijn ingericht (door middel van ontwerp- en standaardinstellingen) dat slechts noodzakelijke persoonsgegevens worden verwerkt voor het beoogde doel en niet langer worden bewaard dan noodzakelijk. Het is belangrijk om hier bij grote wijzigingen of projecten expliciet bij stil te staan en dit ook vast te leggen.

De principes *privacy by design* en *privacy by default* (artikel 25) worden toegepast door de organisatie en geborgd in processen en procedures zoals bijvoorbeeld het change proces en projectenproces. Privacy by design betekent dat bij nieuwe diensten of services privacy meegenomen dient te worden bij de ontwerpkeuzes en criteria. Privacy by default betekent dat standaard de meest strikte privacy settings moeten worden toegepast wanneer er een nieuw product of service wordt geïntroduceerd.

➔ *De RUD Utrecht borgt dit middels interne processen en procedures, en ziet erop toe dat haar leveranciers zich aan dezelfde regels houden. Concreet betekent dit dat de afweging / controle expliciet dient te worden vastgelegd wanneer er iets wijzigt in de verwerking van persoonsgegevens of wanneer er nieuwe systemen / processen ten behoeve van het verwerken van persoonsgegevens worden geïntroduceerd.*

8.3 Anonimisering en pseudonimisering

Puur anonieme gegevens vallen buiten de scope van de AVG. Deze zijn namelijk niet herleidbaar tot een persoon. Bij pseudonimisering ligt dat anders. Pseudonimisering zorgt er namelijk voor dat gegevens niet kunnen worden herleid tot een individu zolang de gegevens geïsoleerd worden beschouwd. Dit betekent dat de herleidbaarheid is beperkt, maar niet voorgoed onmogelijk is gemaakt. Met behulp van “aanvullende informatie” zijn gepseudonimiseerde gegevens wederom te herleiden naar persoonsgegevens. Om deze reden worden pseudonieme persoonsgegevens door de AVG gezien als persoonsgegevens, waardoor de AVG op dergelijke gegevens onverminderd van toepassing is. Overigens worden beide methoden door de AVG gezien als belangrijke maatregel om persoonsgegevens te beschermen. Dit wordt doorgaans het meest expliciet in het geval van testdata.

8.3.1 Testdata en anonimisering

Het selecteren en gereed maken van datasets met testdata is een tijdrovend karwij. Testdata moet juist, volledig en productie-like zijn, zodat uitgevoerde testen met deze data ook representatief zijn. Aanvullend stelt de AVG data testdata niet zomaar een kopie van de productie-data mag zijn, omdat er anders sprake kan zijn van een ‘onrechtmatige verwerking’ (er wordt dan voorbij gegaan aan het doel en de grondslag van de verwerking) en/of een ‘verhoogd risico op lekken’.

Onrechtmatige verwerking omdat het testen door een verwerker (zoals bijvoorbeeld de RUD Utrecht) geen onderdeel is van de door de verantwoordelijke (de klanten van de RUD Utrecht) bepaalde doelen op basis waarvan de persoonsgegevens door de RUD Utrecht mogen worden verwerkt. Doelen worden namelijk geformuleerd binnen de context van primaire bedrijfsprocessen, en dat betekent dat de persoonsgegevens niet zomaar door de verwerker mag worden gebruikt voor ondersteunende processen (zoals testen). Het door verwerkingsverantwoordelijke opnemen van ‘testen’ als onderdeel van het doel van de verwerking, is helaas geen optie. Zoals beschreven in hoofdstuk 8.2 verlangt de AVG van de verwerkingsverantwoordelijke dat deze kan aantonen dat de verwerking zoveel als mogelijk wordt beperkt (*privacy by design* en *privacy by default*), waardoor het moeilijk is om te verdedigen dat het testen door verwerker wordt gezien als doel van de verwerking vanuit de verwerkingsverantwoordelijke.

➔ *Omdat het gebruiken van echte persoonsgegevens in test- of acceptatieomgeving buiten het doel van de verwerking vallen, dienen persoonsgegevens in dergelijke omgevingen te worden geanonimiseerd of gepseudonimiseerd. Het is de verantwoordelijkheid van de RUD Utrecht om hierop toe te zien; ook bij haar leveranciers.*

➔ *Wanneer een leverancier van de RUD Utrecht uitsluitend gepseudonimiseerde persoonsgegevens verwerkt, dan is de AVG onverminderd van toepassing. Er dient dan bijvoorbeeld een verwerkersovereenkomst te worden afgesloten.*

8.4 Encryptie

Het toepassen van encryptie wordt gezien als een belangrijke maatregelen om persoonsgegevens te beschermen. Het is dan uiteraard wel belangrijk om de kosten hiervan goed af te wegen tegen het risico. Ook dient er een onderscheid te worden gemaakt tussen encryptie at rest en encryptie in transit. Het zogenaamde cryptografisch beleid is een onderdeel van het informatiebeveiligingsbeleid van de RUD Utrecht. Hierin staat beschreven aan welke cryptografische eisen de (externe) ICT omgeving dient te voldoen.

Vanuit de AVG beredeneerd wordt encryptie van persoonsgegevens gelijk gesteld aan het pseudonimiseren van persoonsgegevens. Met de encryptiesleutel is het immers mogelijk om de versleutelde gegevens weer te herleiden naar persoonsgegevens. De encryptiesleutel is daarom vergelijkbaar met de “aanvullende gegevens” die binnen een pseudonimiseringscontext gebruikt kunnen worden om gepseudonimiseerde gegevens te herleiden naar persoonsgegevens.

➔ *De RUD Utrecht dient te borgen dat zij op de juiste plekken encryptie toepast om zodoende een passende vertrouwelijkheid en integriteit van persoonsgegevens te realiseren. Mogelijk is hiervoor een inventarisatie nodig. Bijvoorbeeld op basis van technische en logische ontwerpdocumentatie, of op basis van analyse van werkprocedures.*

➔ *Wanneer een leverancier van de RUD Utrecht uitsluitend versleutelde (encryptie) persoonsgegevens verwerkt, dan is de AVG onverminderd van toepassing. Er dient dan bijvoorbeeld een verwerkersovereenkomst te worden afgesloten.*

8.5 Aantonen door certificering

Volgens de AVG is certificering één van de middelen om te laten zien dat een organisatie passende technische en organisatorische maatregelen heeft genomen. Het is op moment van schrijven echter nog niet duidelijk welke certificeringen er worden gezien als voldoende.

9 Overeenkomst

Bij het uitbesteden van een verwerking of bij het verwerken van persoonsgegevens van een andere partij moeten afspraken worden gemaakt tussen de verwerkingsverantwoordelijke en de verwerker. Deze afspraken kunnen worden vastgelegd in een overeenkomst die 'verwerkersovereenkomst' wordt genoemd[2]. Dit is een gangbare, maar geen officiële term uit de AVG. De afspraken kunnen ook volgen uit een andere rechtshandeling krachtens Unierecht of lidstatelijke recht. Van belang is dat onder meer verantwoordelijkheden worden benoemd, bijvoorbeeld bij wie de regie berust en waar betrokkenen een aanspreekpunt kunnen vinden met betrekking tot de verwerking.

Bij gegevensuitwisseling tussen twee verwerkingsverantwoordelijken is het eveneens aan te bevelen een overeenkomst te sluiten waarin de betrokken partijen afspraken over de gegevensdeling vastleggen, bijvoorbeeld dat de deling van de gegevens rechtmatig is en veilig plaatsvindt. Er moet altijd een geldige grondslag zijn voor het verwerken van de persoonsgegevens. Dit betekent dat persoonsgegevens niet mogen worden gebruikt voor een ander doel dan in de overeenkomst is vastgelegd (bijvoorbeeld een kopie van productiedata in een testomgeving), tenzij de overeenkomst hier expliciet voor wordt aangepast. De ontvangende partij is zelf verantwoordelijk voor de technische en organisatorische maatregelen die voor de beveiliging van de gegevens nodig zijn.

Volgens de AVG wordt in een verwerkersovereenkomst minimaal het volgende geregeld:
- Het doel van de verwerking (doelbinding);

[2] Een verwerkersovereenkomst vloeit voort uit privacywetgeving. Wanneer er geen persoonsgegevens worden verwerkt, is een verwerkersovereenkomst dus niet nodig.

- Persoonsgegevens mogen uitsluiten worden verwerkt op basis van schriftelijke instructies van de verantwoordelijke;
- Personen betrokken bij de verwerking borgen vertrouwelijkheid door bijvoorbeeld het ondertekenen van een NDA of een geheimhoudingsclausule als onderdeel van de arbeidsovereenkomst;
- De technische en organisatorische maatregelen die door de verwerker worden genomen zijn vastgelegd in een bijlage;
- Of er sprake is van algemene of specifieke toestemming voor het inschakelen van sub-verwerkers door verwerker;
- Dat er met de sub-verwerker door verwerker een sub-verwerkersovereenkomst wordt gesloten die voldoet aan de AVG;
- Of en, zo ja, hoe verwerker de verwerkingsverantwoordelijke bijstaat in het geval betrokkenen hun rechten ingevolge de AVG wensen uit te oefenen;
- Of en, zo ja, hoe verwerker de verwerkingsverantwoordelijke bijstaat bij:
    - Beveiliging van de verwerking;
    - Melding inbreuken aan Autoriteit Persoonsgegevens (datalekken);
    - Mededeling inbreuken aan betrokkenen;
    - Gegevensbeschermingseffectbeoordeling (DPIA);
    - Indien nodig: voorafgaande raadpleging Autoriteit Persoonsgegevens.
- Na afloop van de verwerking worden persoonsgegevens gewist en indien de verwerkingsverantwoordelijke dit wenst, eerst teruggegeven aan de verwerkingsverantwoordelijke;
- Verwerkingsverantwoordelijke stelt alle informatie ter beschikking die nodig is om de nakoming van de verplichtingen onder de AVG aan te tonen;
- De verwerker laat audits door de verwerkingsverantwoordelijke, of door een door verwerkingsverantwoordelijke aangewezen auditor, toe om te controleren of verwerker aan de verplichtingen ingevolgde de AVG en verwerkersovereenkomst voldoet of heeft voldaan;
- De verwerker stelt verwerkingsverantwoordelijke onmiddellijk op de hoogte wanneer verwerker van mening is dat een instructie van de verwerkingsverantwoordelijke in strijd is met de AVG;
- Of verwerker gecertificeerd is, zodat hiermee kan worden aangetoond dat verwerker voldoende garanties biedt.

Verwerkingen worden geregeld in overeenkomsten (artikel 28) en in deze overeenkomsten worden concrete beveiligingsafspraken gemaakt (artikel 32).

➔ *Omdat de RUD Utrecht ook persoonsgegevens verwerkt of laat verwerken, is het noodzakelijk om verwerkersovereenkomsten met leveranciers of partners af te sluiten, en hierin goede en expliciete afspraken te maken over de beveiliging van de persoonsgegevens. Hiervoor kan een richtlijn beveiligingsafspraken derden worden opgesteld.*

In de praktijk wordt op grote schaal gewerkt met verwerkers, ook door de overheid. De verwerkingscontracten die hierbij in de regel worden opgesteld, zullen, vanaf het moment van het van kracht worden van de verordening, moeten voldoen aan de vereisten beschreven in dit hoofdstuk.

➔ *RUD Utrecht past bestaande overeenkomsten aan, zodat deze voldoen de AVG vereisten.*

9.1 Verwerker of niet?

In veel gevallen kan een leverancier worden gezien als een verwerker, maar er kunnen ook situaties zijn waarin een leverancier niet voldoet aan de criteria voor verwerker, maar optreed als verwerkingsverantwoordelijke. Met andere woorden: de relatie opdrachtgever/opdrachtnemer is niet hetzelfde dan de relatie verwerkersverantwoordelijke/verwerker. Dit zijn twee verschillende dingen die geen directe relatie met elkaar hebben. Dit betekent dat een relatie tussen de RUD Utrecht en haar leveranciers ook een relatie tussen twee verwerkingsverantwoordelijken kan zijn.

De AVG beschrijft dat de verwerkingsverantwoordelijke het 'doel' en de 'middelen' (het 'waarom' en het 'hoe') voor de verwerking van persoonsgegevens vaststelt (artikel 4.7). Een verwerker is een partij die ten behoeve van een ander (de verwerkingsverantwoordelijke) persoonsgegevens verwerkt. In deze relatie zijn de partijen verplicht hun relatie contractueel te regelen met een zogeheten verwerkersovereenkomst. De verantwoordelijke is wettelijk aansprakelijk voor hetgeen de verwerker doet, zodat het belangrijk is deze posities goed te bepalen.

9.1.1 Criteria voor verwerker

De bepaling of een partij een verwerker is, moet gebeuren aan de hand van de feitelijke/werkelijke situatie. Primair is hierbij van belang in welke mate een partij invloed kan uitoefenen op de doelen van de verwerking. Secundair is de invloed van een partij op de middelen van de verwerking. Wanneer bijvoorbeeld de klant het doel bepaalt en de leverancier de middelen, is niet meteen duidelijk of een leverancier als verwerker is te zien. In een dergelijk geval geeft de doelbepalende partij (de klant) de doorslag. Er kan worden gesteld dat de doelbepalende partij (de klant) de middelen van de leverancier (de partij die de middelen bepaalt) goedkeurt, en ze daarmee heeft vastgesteld. De klant is dan verwerkingsverantwoordelijke en de leverancier verwerker.

De feitelijke/werkelijke situatie kan worden geanalyseerd aan de hand van 3 factoren: mate van beslisbevoegdheid, mate van inspraak, en positie van de andere partij. Deze factoren worden hieronder nader toegelicht, en per factor worden een aantal voorbeeldvragen genoemd die kunnen helpen bij de analyse. Hou hierbij in gedachte dat dit geen exacte wetenschap is, en dat voldoende juridische kennis én correcte interpretatie van terminologie nodig zijn voor een analyse die kwalitatief volstaat.

De voorbeeldvragen zijn geformuleerd vanuit het perspectief van de andere partij, niet zijnde de RUD Utrecht.

Mate van beslisbevoegdheid - de hoeveelheid ruimte die de andere partij krijgt/heeft om zelf te beslissen hoe de verwerking wordt uitgevoerd, is een sterke indicatie van verwerkerschap. Wanneer de andere partij een hoge mate van beslisbevoegdheid heeft, dan neemt de waarschijnlijkheid toe dat deze partij optreed als verwerkingsverantwoordelijke.

- Welke mate van zeggenschap heeft de andere partij bij de verwerking?
    - Bepaalt de RUD Utrecht volledig hoe de andere partij te werk moet gaan, of neemt de RUD Utrecht een dienst af zonder invloed te hebben op hoe dit gaat gebeuren?
- Wat gebeurt er met de resultaten van de verwerking?
    - Worden de resultaten uitsluitend aan de RUD Utrecht beschikbaar gesteld, of worden de resultaten door de andere partij ook gebruik voor de eigen dienstverlening en worden er alleen algemene resultaten aan de RUD Utrecht gerapporteerd?
- Wat bepaalt het contract tussen de RUD Utrecht en de andere partij over eigendom van persoonsgegevens?
    - Blijft de RUD Utrecht eigendom van de persoonsgegevens, of worden de persoonsgegevens eigendom van de andere partij?

Mate van inspraak - de hoeveelheid invloed die de andere partij heeft op de doelen van de verwerking. Als er geen inzicht is in wat de partij met de gegevens gaat doen, dan is een verwerkersrelatie onwaarschijnlijk. Dat maakt een verwerkersrelatie onwaarschijnlijk. Daarbij komt dat u deze partij contractueel noch praktisch zou kunnen stoppen als zij zelfgekozen doelen gaan uitvoeren. Dit is typisch voor een verantwoordelijke.

- Hoe kan de verwerking het beste worden omgeschreven?
    - Bij bepaalde type verwerkingen is de andere partij doorgaans als verwerkingsverantwoordelijke aan te merken.
        - Uitvoerders van een wettelijke taak. Accountant, notaris, advocaat. Deze uitvoerders mogen niet worden gezien als verwerker omdat zij zelf bepalen hoe de taak wordt uitgevoerd.

        - PostNL ziet zichzelf ook niet als verwerker: zij vinden dat ze zélf bepalen waar de post heen gaat en wat ze doen met persoonsgegevens, bv. de ontvanger via hun app informeren over de voortgang. Ook kunnen ze dan bijvoorbeeld statistieken over klanten heen uitvoeren, wat waarschijnlijk de achterliggende reden is.
- In hoeverre is bekend wat de andere partij gaat doen met de persoonsgegevens?
    - Als de RUD Utrecht weet wat de andere partij met de persoonsgegevens gaat doen en hier invloed op kan uitoefenen, dan is de andere partij waarschijnlijk verwerker.
    - Als de RUD Utrecht geen zicht heeft op wat de derde partij met de persoonsgegevens doet en hier ook geen/weinig invloed op kan uitoefenen, dan is de andere partij waarschijnlijk verwerkersverantwoordelijke.
- Kunnen de door de andere partij gekozen doelen worden tegengehouden of beïnvloed?
    - De RUD Utrecht kan hier praktisch noch contractueel iets tegen doen.
    - De andere partij mag niks op eigen initiatief met de persoonsgegevens doen.
    - De RUD Utrecht heeft de mogelijkheid de andere partij een halt toe te roepen op het moment dat de verwerking niet wenselijk is.

Positie van de andere partij - het gaat hier om een derde partij, die zelf zijn bedrijfsvoering inricht en waar u niet direct zicht op zult hebben. Het is daarmee goed mogelijk dat deze partij toch een verantwoordelijke is. Het contract bepaalt verder nog dat deze partij is, wat een zeer sterke aanwijzing die kant op is maar niet doorslaggevend. Het gaat namelijk uiteindelijk om de werkelijke situatie.

- Welke band is er tussen de RUD Utrecht en de andere partij?
    - Als de derde partij een zelfstandige organisatie is, die zelf beslist hoe ze haar bedrijfsvoering inricht, is dat een indicatie voor verwerkingverantwoordelijkheid.
- Wat bepaalt het contract over verwerkerschap?
    - Wat het contract bepaalt is een indicatie, maar niet doorslaggevend. Het gaat namelijk om de feitelijke/werkelijke situatie.

➔ *Een leverancier die in opdracht van de RUD Utrecht werkt met persoonsgegevens van de RUD Utrecht of haar klanten, wordt gezien als verwerker tenzij zonder enige twijfel wordt vastgesteld dat de leverancier optreed als verwerkingsverantwoordelijke.*

➔ *Wanneer er geen verwerkersovereenkomst nodig is, dienen er wel andere contractuele afspraken te worden gemaakt over de dienstverlening. Waaronder in ieder geval afspraken over informatiebeveiliging.*

9.2 RUD als gezamenlijke regeling: verwerker of verwerkingsverantwoordelijke

De RUD Utrecht is een gemeenschappelijke regeling (GR) die taken uitvoert die bij wet aan haar klanten (gemeenten) zijn toegekend. Om te bepalen of de RUD Utrecht in verhouding tot haar klanten (gemeente) als verwerker of verwerkingsverantwoordelijke optreed, kan in eerste instantie worden gekeken naar de wijze waarop de taken aan de RUD zijn toegekend.

In het geval van *mandaat* of *machtiging* worden de bevoegdheden door de RUD Utrecht namens de gemeenten uitgeoefend. In principe blijven de gemeenten in een dergelijke situatie verwerkingsverantwoordelijke (en de RUD Utrecht verwerker), maar er kan ook sprake zijn van een gezamenlijke verantwoordelijkheid wanneer de RUD Utrecht feitelijk/werkelijk invloed uitoefent op het doel en middelen van de verwerking. Kortom, de feitelijke/werkelijke mate van invloed dient te worden vastgesteld op basis van de criteria in 9.1.1, zodat op basis van het ontstane inzicht kan worden bepaald of de RUD Utrecht richting haar klanten (gemeenten) optreed als verwerker of verwerkingsverantwoordelijke.

In het geval van *delegatie van bevoegdheden* is de RUD Utrecht zelfstandig bevoegd gemaakt om de overgedragen bevoegdheden uit te oefenen en is de RUD Utrecht bestuurlijk verantwoordelijke. In

principe is de RUD Utrecht dan als verwerkingsverantwoordelijke aan te merken, maar ook in deze situatie dient er te worden gekeken naar de feitelijke/werkelijke situatie. Wanneer de gemeenten in de praktijk bijvoorbeeld zelf het doel en de middelen van de verwerking geheel of gedeeltelijk vaststellen, dan is de RUD Utrecht mogelijk toch verwerker of is er sprake van een gedeelde verantwoordelijkheid. Ook in dit geval kunnen de criteria in 9.1.1 worden gebruikt om vast te stellen of de RUD Utrecht richting haar klanten (gemeenten) optreed als verwerker of verwerkingsverantwoordelijke.

10 Functionaris gegevensbescherming

Een functionaris gegevensbescherming (FG), ook wel Data Protection Officer (DPO) genoemd, houdt toezicht op de toepassing en naleving van de AVG binnen een organisatie. Het aanstellen van een functionaris gegevensbescherming is verplicht in drie gevallen:

1. voor overheden en publieke organisaties;
2. voor organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen/observeren;
3. voor organisaties die vanuit hun kernactiviteit op grote schaal bijzondere persoonsgegevens verwerken.

Het hebben van een personeelsbestand voor bijvoorbeeld salarisverwerking of IT helpdesk doeleinden worden gezien als een ‘ancillary function’ (ondersteunende taak / nevenactiviteit) in plaats van een ‘core activity’ (kernactiviteit). Hierdoor is het hebben van een personeelsadministratie doorgaans geen argument om verplicht een functionaris gegevensbescherming aan te stellen.

Ten aanzien van een functionaris gegevensbescherming geldt het volgende:

- De wettelijke taken en bevoegdheden van de FG geven hem/haar een onafhankelijke positie in de organisatie.
- De FG moet een natuurlijk persoon zijn.
- De FG dient aangemeld te worden bij de Autoriteit Persoonsgegevens[3].
- De FG functie kan ook worden bekleed op basis van een dienstverleningsovereenkomst die werd afgesloten met een persoon of een organisatie die niet tot de organisatie van de verwerkingsverantwoordelijke / verwerker behoort.
- Organisaties mogen op vrijwillige basis een FG aanwijzen. Voor een vrijwillige FG gelden na aanstelling dezelfde rechten en plichten dan voor een verplichte FG.
- Een FG is niet persoonlijk verantwoordelijk bij niet-naleving van de AVG.
- Een FG geniet ontslagbescherming, vergelijkbaar met leden van de ondernemingsraad. Beëindiging van de arbeidsovereenkomst in relatie tot de uitvoering van specifieke FG taken, kan alleen middels de kantonrechter.

➔ *De RUD Utrecht is verplicht tot het aanstellen van een functionaris gegevensbescherming, omdat zij een openbaar lichaam is, en daarmee een onderdeel van de Nederlandse overheid.*

11 Persoonsgegevens buiten Europa

Volgens de Europese privacywet is het verboden om zonder aanvullende afspraken, persoonsgegevens te laten verwerken door landen buiten de Europese Unie. Achterliggende gedacht is dat de lokale wetten in dergelijke landen onvoldoende waarborgen bieden voor de bescherming van de persoonsgegevens. Ook de Verenigde Staten wordt door de Europese Commissie aangemerkt als een land zonder passend beschermingsniveau. Dat komt doordat de Amerikanen de privacy van buitenlanders niet of nauwelijks beschermen. De Amerikaanse privacywetgeving geldt op dit moment alleen voor inwoners van de VS, waardoor er geen juridische grondslag is voor de bescherming van buitenlanders. Onder druk van de internationale gemeenschap beloven de Amerikanen al langere tijd de nodige verbeteringen, maar deze komen niet of nauwelijks op gang.

[3] Aanmelden kan met behulp van dit formulier:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/aanmelding_fg.pdf

Aangezien veel organisaties gebruik maken van de diensten van Amerikaanse (cloud)leveranciers, is het voor organisaties binnen de Europese Unie belangrijk om te zorgen dat de er aanvullende afspraken worden gemaakt waarmee de bescherming van de persoonsgegevens voldoende wordt beschermd. Door gebruik te maken van Europese modelcontracten kan dit worden geregeld. Specifiek voor Amerikaanse leveranciers kan er naast het gebruik van Europese modelcontracten ook gebruik worden gemaakt van het EU-US Privacy Shield. Beide mogelijkheden worden hieronder nader toegelicht.

11.1 Europees Modelcontract

Voor het exporteren van persoonsgegevens naar landen buiten de Europese Unie zonder passend beschermingsniveau kan ook gebruik worden gemaakt van ongewijzigde (!) modelcontracten die door de Europese Commissie zijn opgesteld. Deze contracten bieden op dit moment nog een rechtmatige oplossing, maar de verwachting is dat deze op termijn ongeldig worden verklaard door het Europese Hof van Justitie, aangezien deze modelcontracten onvoldoende waarborgen zouden vormen voor de bescherming van persoonsgegevens. Vooralsnog is daarvan echter nog geen sprake, dus kunnen de modelcontracten worden gebruikt. Hieronder een aantal links naar verschillende modelcontracten:

- Doorgifte tussen twee verantwoordelijken waarvan een binnen en een buiten de Europese Unie;
- Een alternatief op bovengenoemd modelcontract opgesteld door het bedrijfsleven;
- Doorgifte van persoonsgegevens vanuit Europese Unie aan in derde landen gevestigde verwerkers.

Wanneer modelcontracten met een aanvulling of wijziging worden gebruikt, dan dient er voor het gebruik van de aangepaste versie een vergunning bij de Autoriteit Persoonsgegevens te worden aangevraagd.

11.2 EU-U.S. Privacyschild (vervanger Safe Harbor)

Om uitwisseling van persoonsgegevens tussen Europese organisaties en Amerikaanse leveranciers mogelijk te maken, werd in 2000 het Safe Harbor framework opgezet. Door zelfcertificering kon een leverancier stellen zich te houden aan de zogenaamde ‘Safe Harbor Principles’, waarna doorgifte van persoonsgegevens was toegestaan. Deze papieren exercitie bood echter geen enkele garantie, en voldeed ook niet aan destijds geldende Nederlandse privacywet. Deze vereiste namelijk dat er een bewerkersovereenkomst werd opgesteld en dat er expliciete afspraken t.a.v. de beveiliging van de gegevens worden gemaakt. Verschillende critici waren al langer van mening dat het Safe Harbor framework alleen maar een juridische cover-your-ass constructie bood, en in werkelijkheid onvoldoende concrete waarborgen bood voor de bescherming van (persoons)gegevens.

In oktober 2015 werd het Safe Harbor framework door het Europese Hof van Justitie ongeldig verklaard. De Europese privacytoezichthouders gaven de Europese Commissie tot 31 januari 2016 de tijd om nieuwe afspraken te maken met de Verenigde Staten over adequate bescherming van data van Europese burgers. Hierna zouden ze gaan ingrijpen en dat zou vergaande consequenties kunnen hebben voor organisaties in Europa.

Begin februari 2016 berichtte de Europese Commissie dat er een overeenkomst is bereikt die de naam ‘EU-U.S. Privacy Shield’ draagt. Na het doorvoeren van een aantal verbeteringen in de concept versie, heeft de Europese Commissie de definitieve versie op 12 juli 2016 gepubliceerd. Vanaf 1 augustus 2016 kunnen Amerikaanse organisaties middels zelfcertificering aangeven te voldoen aan de geldende privacyeisen, en hun certificering indienen bij het Amerikaanse ministerie van Handel. Wanneer laatstgenoemde de desbetreffende Amerikaanse organisatie opneemt in het register van het Privacy Shield, mogen Europese organisaties persoonsgegevens doorgeven naar deze Amerikaans organisatie.

Over de toekomstvastheid van het EU-US Privacy Shield bestaan nog twijfels. Critici zijn van mening dat het EU-US Privacy Shield (nog steeds) onvoldoende bescherming biedt, en verwachten dat het Europese Hof van Justitie ook deze nieuwe overeenkomst ongeldig verklaard.

➔ *De RUD Utrecht dient te borgen dat wanneer zij persoonsgegevens laat verwerken door organisaties buiten Europa:*
- *dat er een Europees modelcontract is afgesloten, of*

- *in het geval van Amerikaanse bedrijven, dat deze bedrijven zijn opgenomen in het EU-U.S. Privacy Shield.*

11.3 Gag Order risico

Ondanks de mogelijkheden om het verwerken van persoonsgegevens door Amerikaanse organisaties vanuit een juridisch oogpunt te legaliseren, is er nog steeds sprake van een risico dat ontstaat doordat de Amerikaanse wet conflicteert met Europese wetgeving. Dit risico is onder andere bekend als het zogenaamde Gag Order risico, en het is belangrijk dat organisaties dit risico bewust adresseren.

Als gevolg van onder andere de Patriot Act en FISA wetgeving kan de Amerikaanse overheid data bij Amerikaanse leveranciers opvragen zonder dat deze hier de data-eigenaar over mogen informeren (een zogenaamde Gag Order). Het feit dat een dergelijke leverancier een datacenter in Europa heeft en de data alleen maar in dat datacenter opslaat, doet daar niets aan af. Zolang het een Amerikaanse leverancier betreft, of wanneer de dataopslag om andere redenen onder Amerikaanse jurisdictie valt, kan de Amerikaans overheid zonder medeweten van de data-eigenaar alle data opvragen ongeacht de (fysieke) opslaglocatie. De Amerikaanse wet en de Europese wet zijn op dit vlak dus conflicterend, en Amerikaanse leveranciers staan feitelijk voor een onmogelijke keuze: voldoen aan Europese wetgeving of aan Amerikaanse wetgeving.

In een iets andere context geldt dit overigens ook voor medewerkers met een Amerikaans paspoort in dienst van een Europese organisatie, waaronder ook medewerkers met een dubbele nationaliteit. Omdat Amerikanen worden verondersteld vaderlandslievend te zijn (Patriot Act), is het wettelijke uitgangspunt dat Amerikaanse medewerkers van de Amerikaanse overheid opdracht kunnen krijgen om data van de werkgever te lekken aan de Amerikaanse overheid. Ook hier weer zonder medeweten van de organisatie waar de medewerker in dienst is. Vanuit Amerikaanse wetgeving en als gevolg van het hebben van een Amerikaans paspoort, zijn dergelijke medewerkers verplicht om aan dergelijke verzoeken van de Amerikaanse overheid gehoor te geven. Afhankelijk van de risicobereidheid betekent dit, dat je als organisatie eigenlijk dient te weten of je medewerkers (en misschien ook wel de medewerkers van je leveranciers) meerdere nationaliteiten hebben en, zo ja, of hier dan een Amerikaanse nationaliteit tussen zit. Hier zitten ook mogelijke conflicten in wetgeving, want iemand weigeren aan te nemen op basis van nationaliteit valt onder discriminatie en is strafbaar.

Het komt er in ieder geval op neer dat er (nog) geen structurele oplossing bestaat voor het Gag Order risico. Zolang er data wordt opgeslagen op servers onder Amerikaanse jurisdictie, kan de Amerikaanse overheid beschikken over deze gegevens. Er is geen wet of regel die dit voorkomt, maar er ontstaat steeds meer weerstand vanuit Amerikaanse leveranciers. Microsoft bijvoorbeeld is in VS verwikkeld in diverse rechtszaken, omdat ze de Amerikaanse overheid geen toegang willen geven tot klantdata op basis van een Gag Order. Ook heeft Microsoft in samenwerking met het Duitse T-Systems International een separate Azure cloud in Duitsland opgezet die juridisch gezien buiten het bereik van Amerikaanse wetgeving valt. De Amerikaanse overheid kan dan niet meer middels een Gag Order over de gegevens in deze cloud beschikken. Hiermee kan worden voldaan aan Europese wetgeving.

➔ *De RUD Utrecht dient te besluit hoe om te gaan met het verwerken van persoonsgegevens door derden waardoor de gegevens onder Amerikaanse jurisdictie vallen. De eisen en wensen van klanten kunnen hierin voor de RUD Utrecht leidend zijn.*

12 Overige verplichtingen vanuit de AVG

Om te voldoen aan de AVG dient de RUD Utrecht invulling te geven aan een aantal verantwoordelijkheden. In dit document zijn de meest voorname verantwoordelijkheden reeds benoemd. Dit hoofdstuk geeft een beknopt overzicht van de taken die ten behoeve van deze verantwoordelijkheden uitgevoerd dienen te worden.

Organisaties hebben een documentatieplicht (artikel 30). Dit betekent onder andere dat organisaties moeten kunnen aantonen wat voor informatie zij opslaan of verwerken, van wie deze data is, waar dit wordt opgeslagen en hoe dit is beveiligd. Er wordt een register bijgehouden waarin dit wordt

vastgelegd. Voorbeelden: personeelsadministratie, nieuwsbrief, klanten, leveranciers, website bezoekers.

➔ *Er wordt door de RUD Utrecht een verwerkingsregister bijgehouden waarin alle verwerkingen zijn gedocumenteerd.*

Organisaties met vestigingen in meerdere EU-lidstaten hoeven nog maar met één toezichthouder zaken te doen. Namelijk degene in het land waar de hoofdvestiging is gevestigd (artikel 56).

➔ *De RUD Utrecht handelt haar zaken af met de Autoriteit Persoonsgegevens in Nederland.*

13 Compliance risico's

Het niet voldoen aan de bepalingen uit de AVG vormt een risico. De Autoriteit Persoonsgegevens kan aan verwerkingsverantwoordelijken een boete van maximaal €10 miljoen of, indien dat bedrag hoger uitkomt, 2% van de wereldwijde jaaromzet opleggen wanneer de verwerkingsverantwoordelijke de verplichtingen die voortvloeien uit de AVG niet nakomt. Wanneer de verwerkersverantwoordelijke de beginselen of grondslagen van de AVG overtreedt, of de privacyrechten van betrokkenen schendt, dan kan de Autoriteit Persoonsgegevens aan verwerkingsverantwoordelijken een boete van maximaal €20 miljoen of, indien dat bedrag hoger uitkomt, 4% van de wereldwijde jaaromzet opleggen.

Een boete door de handhavende instantie is echter niet het enige risico als volg van onzorgvuldige omgang met persoonsgegevens. In de volgende paragrafen volgen nog een aantal voorbeelden van mogelijke risico's binnen een AVG context.

13.1 Voorbeelden van risico's voor de organisatie

- Negatieve publiciteit en imagoschade.
- Dwangmaatregelen of boetes opgelegd door de toezichthouder wegens het niet naleven van de wetgeving.
- Schadeclaims door betrokkenen.
- Hogere kosten bij het achteraf nemen van privacy maatregelen.
- Slechte datakwaliteit leidt tot slechtere performance van de business.
- Datalekken leiden tot wantrouwen.

13.2 Voorbeelden van juridische risico's

- Niet naleving van privacy regelgeving.
- Niet naleving van sectorale regelgeving.
- Niet naleving van mensenrechten.

13.3 Voorbeelden van risico's voor de betrokkene

- De mogelijkheid om anoniem gebruik te make van bepaalde diensten wordt gefrustreerd.
- Persoonsgegevens worden gedeeld en gebruikt op onrechtmatige wijze.
- Persoonsgegevens worden gebruikt voor doeleinden waar de betrokkenen niet van op de hoogte zijn.
- Het koppelen van systemen kan ertoe leiden dat meer persoonsgegevens worden gebruikt dan noodzakelijk.
- Kwetsbare groepen personen worden eerder het slachtoffer van oneigenlijk gebruik van hun persoonsgegevens en kunnen hierdoor gevolgen van ondervinden als uitsluiting, discriminatie of stigmatisering.
- persoonsgegevens worden niet of onjuist gemanaged waardoor er een wildgroei aan bestanden met persoonsgegevens ontstaat; hierdoor stijgen de veiligheidsrisico's.

14 Bronnen

Bij het opstellen van dit privacybeleid zijn de onderstaande bronnen geraadpleegd.

- CIP Privacy Baseline v3.0: https://www.cip-overheid.nl/wp-content/uploads/2017/05/20170509%20Privacy%20Baseline%20v3_0.pdf
- Boek: “De Algemene Verordening Gegevensbescherming Editie 2017” door Arnoud Engelfriet, Lisette Meij, Peter Kager. ISBN: 9789082083446. Eerste druk.
- Whitepaper AVG – GDRP van Stimmt B.V.
- Factsheet meldplicht datalekken: https://ictrecht.nl/factsheets/impact-van-de-meldplicht-datalekken/
- PIA vragenlijst door Norea: https://www.norea.nl/download/?id=522
- https://www.baaten.com/kennis/wet-en-regelgeving-informatiebeveiliging/europese-privacywet-avg/
- https://ictrecht.nl/2017/01/05/artikel-29-werkgroep-richtlijnen-functionaris-gegevensbescherming-fg/
- Guideline on Data Protection Officers: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp243_rev01_enpdf_0.pdf
- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/functionaris-voor-de-gegevensbescherming-fg
- https://www.baaten.com/kennis/wet-en-regelgeving-informatiebeveiliging/persoonsgegevens-buiten-europa/
- http://dirkzwagerieit.nl/2017/12/13/uitvoeringswet-avg-uavg-gepubliceerd-eerste-analyse/
- Wetsvoorstel Uitvoeringswet Algemene Verordening Gegevensbescherming
- Memorie van toelichting op het wetsvoorstel van de Algemene Verordening Gegevensbescherming
- Ontslagbescherming: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming
- https://cms.law/nl/NLD/Publication/Privacy-de-begrippen-verantwoordelijke-en-bewerker-nader-uitgelegd
- Opinion 1/2010 on the concepts of "controller" and "processor" – http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf
- https://www.it-jurist.nl/nieuws/testen-met-productie-data-mag-dat
- https://www.nederlandict.nl/news/avg-uitgelegd-deel-3-privacy-by-design-privacy-by-default/
- Guidelines DPIA door WP29- https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp248_rev.01_nl.pdf
- https://www.kneppelhout.nl/actueel/wanneer-is-een-data-protection-impact-assessment-dpia-vereist
- https://www.vijverbergjuristen.nl/publicaties/gemeenschappelijke-regeling-verwerkingsverantwoordelijke-of-verwerker-als-bedoeld-in