Implementatie Algemene verordening gegevensbescherming (AVG)

Inhoudsopgave

1 Inleiding

Op 25 mei 2016 is de Europese Algemene Verordening Gegevensbescherming (hierna: AVG) in werking getreden. De AVG gaat over de bescherming van persoonsgegevens en vormt samen met de Uitvoeringswet AVG de geldende privacyregelgeving.

In de AVG is een overgangstermijn opgenomen tot 25 mei 2018. Op die datum moeten alle organisaties in de publieke en private sector voldoen aan de AVG. De Wet bescherming persoonsgegevens geldt dan niet meer. Omdat de RUD Utrecht ook persoonsgegevens verwerkt is de AVG ook relevant voor de RUD Utrecht.

Dit implementatieplan beschrijft wat de RUD Utrecht moet doen om te gaan voldoen aan de AVG.

1.1 Achtergrondinformatie

Gemiddeld zit iemand met zijn gegevens in honderden tot duizenden bestanden, zowel van het bedrijfsleven als van de overheid. Iedereen moet erop kunnen vertrouwen dat zijn persoonsgegevens voldoende worden beveiligd. De Europese Unie heeft met het doel om deze gegevens te beschermen de Algemene verordening gegevensbescherming (AVG) opgesteld.

In een eerder stadium is de meldplicht datalekken al van kracht geworden. Ook bij de RUD Utrecht kunnen zich datalekken voordoen. Bijvoorbeeld als gevolg van een verkeerd verzonden e-mailbericht of een hack in de ICT-systemen.
Deze, al bestaande, meldplicht is een van de onderwerpen van de AVG. Blijvende aandacht voor dit onderwerp is vereist. Alle medewerkers van de RUD Utrecht moet zich ervan bewust zijn.

Daarnaast wordt via de AVG de positie van de burger versterkt. Burgers krijgen verbeterde en nieuwe rechten. De AVG gebruikt overigens de term ‘betrokkene’. Die term zal daarom verder gebruikt worden.

De RUD Utrecht krijgt verder te maken met een aantal verplichtingen op het gebied van gegevensbescherming. Aangetoond moet kunnen worden dat de RUD Utrecht zich aan de wet houden (accountability). Zo dient een register opgesteld en bijgehouden te worden met daarin een overzicht van alle verwerkingen die de RUD Utrecht doet. Daarnaast moet een Functionaris gegevens-bescherming worden aangesteld. Verder moet voor sommige gegevensverwerkingen eerst een privacy impact analyse worden uitgevoerd.

De Autoriteit Persoonsgegevens, hierna: AP) krijgt uitgebreidere sanctiemogelijkheden (bestuurlijke boete). De boetes kunnen oplopen tot maximaal 10 miljoen voor het schenden van verplichtingen (zoals documentatieplicht) en tot maximaal 20 miljoen voor het schenden van de grondbeginselen van de AVG.

1.2 Uitgangspunten

Een aantal beginselen vormen de rode draad voor het voldoen aan de AVG. Iedere maatregel die we moeten treffen is terug te voeren op deze beginselen:

- Rechtmatigheid: de verwerking is rechtmatig
- Transparantie en verantwoording: het is duidelijk en te achterhalen wat we doen (aantoonbaar)
- Doelbinding: persoonsgegevens worden met een duidelijk doel verwerkt (een goede reden)
- Dataminimalisatie en opslagbeperking: Het verwerken is adequaat en ter zake dienend. Verwerking blijft beperkt tot dat wat minimaal nodig is. Gegevens blijven bewaard zolang als nodig.
- Juistheid: gegevens zijn juist en worden zo nodig geactualiseerd.
- Vertrouwelijkheid: gegevens zijn vertrouwelijk en worden goed beveiligd.

1.3 Doelstelling

De doelstelling van het project is om per 25 mei 2018 te voldoen aan de AVG, zowel op het gebied van ICT (beveiligingsmaatregelen), als op juridisch en organisatorisch gebied. Op juridisch gebied betekent dit dat procedures en beleid zijn vastgesteld.

Op organisatorisch en ICT gebied houdt dit in dat benodigde maatregelen vastgesteld en geïmplementeerd zijn. Bij voorkeur wordt het de medewerkers daarbij zo eenvoudig mogelijk gemaakt, bijvoorbeeld door handige standaardinstellingen in te bouwen in de werkprocessen.

Een heel belangrijk doel is te zorgen voor (meer) bewustwording bij medewerkers en managers. Dit is een blijvend aandachtspunt, ook na dit project.

2 Aanpak

2.1 Afbakening

Op grond van de privacyregelgeving dient de RUD Utrecht zorgvuldig met persoonsgegevens om te gaan. Ook al wordt een groot deel van de taken uitgevoerd in mandaat, onder verantwoordelijkheid van een gemeente of de provincie, de RUD Utrecht is zelfstandig aan te merken als de verwerkingsverantwoordelijke in de zin van AVG.

Nadrukkelijk wordt vermeld dat dit project uitsluitend gaat over *persoonsgegevens*. Uiteraard is het van belang dat met alle gegevens (data) van en bij de RUD Utrecht zorgvuldig wordt omgegaan. Daarom wordt binnen de RUD Utrecht ook informatiebeveiligingsbeleid opgesteld en geïmplementeerd. Dit traject heeft sterke overlap met het AVG-project en loopt gelijktijdig.
Een van de voorwaarden van de AVG is dat passende technische en organisatorische maatregelen worden getroffen ter bescherming van persoonsgegevens. Dit aspect wordt beschreven in het

informatiebeveiligingsbeleid van de RUD Utrecht. Om deze reden is het traject tot het opstellen, vaststellen en implementeren van dit beleid aangehaakt bij dit AVG-project.

In de AVG is bepaald dat de verordening uitsluitend van toepassing is op de geheel of gedeeltelijk geautomatiseerde verwerking en op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin opgenomen te worden. Dit betekent dat persoonsgegevens die in niet-geordende vorm in oude archieven (niet-digitaal) aanwezig zijn, niet worden meegenomen in dit project.

We hebben in het kader van de AVG dus vooral te maken met de persoonsgegevens die zijn opgenomen in digitale systemen, zoals Decos en Squit, en in andere bestanden.

De RUD Utrecht heeft te maken met persoonsgegevens van drie typen betrokkenen, namelijk de inwoners van de regio, contactpersonen van rechtspersonen (zowel bij milieu-inrichtingen als bij bedrijven die diensten voor de RUD Utrecht verrichten) en de eigen (oud-)medewerkers.

2.2 Op te leveren producten

Er moet voor worden gezorgd dat de maatregelen die nodig zijn voor de beveiliging van persoonsgegevens zijn ingevoerd. Procedures, overzichten en beleidsregels dienen te zijn opgesteld. Daarnaast moeten medewerkers en managers zich er van bewust zijn dat een veilige en zorgvuldige omgang met persoonsgegevens vereist is.

In 2017 is al begonnen met het schrijven het Informatiebeveiligingsbeleid en Privacybeleid. Het uitgangspunt is daarbij dat de Tactische Baseline Informatiebeveiliging Nederlandse gemeenten (BIG) wordt toegepast. Het beveiligingsbeleid is eind 2017 vastgesteld. Maatregelen die zorgen voor bewustwording binnen de RUD Utrecht zullen in de eerste helft van 2018 actief plaatsvinden en voor regelmatige aandacht geborgd in de reguliere bedrijfsvoeringcyclus. Tevens is begonnen met het inventariseren van de verwerkingen die binnen de RUD Utrecht plaatsvinden om dit in een verwerkingenregister op te nemen.

Een gedetailleerd overzicht van de uit voeren acties zoals aangegeven in het Privacybeleid en de status daarvan is als bijlage bij dit plan gevoegd. De acties op de lijst waar op dit moment geen prioriteit aan wordt gegeven zijn in grijs gemarkeerd.

2.3 Eindresultaat

Concreet moet aan het eind van het project het volgende zijn gerealiseerd:

- Alle medewerkers zijn op de hoogte van de privacyregels en zijn beveiligingsbewust.
- Passende organisatorische en technische maatregelen ter beveiliging van de persoonsgegevens zijn getroffen. Gegevensbeschermingsbeleid (informatiebeveiligingsbeleid) is vastgesteld en geïmplementeerd.
- Medewerkers en externe partijen hebben uitsluitend toegang tot informatie die zij nodig hebben voor het uitvoeren van hun taken. Dit betekent dat sommige gegevens zijn afgeschermd.

- Beoordeeld is of voor verwerkingen binnen de RUD Utrecht een Privacy impact analyse DPIA noodzakelijk is. Indien noodzakelijk is deze uitgevoerd.
- Een Functionaris Gegevensbescherming is aangesteld.
- Verwerkingen binnen de RUD Utrecht zijn in kaart gebracht en in een register opgenomen.
- Mogelijkheden tot dataminimalisatie zijn beschouwd en doorgevoerd waar nodig.
- Een register voor datalekken is gemaakt en een procedure voor het melden is opgesteld.
- Met opdrachtgevers en dienstverleners van de RUD Utrecht zijn verwerkersovereenkomsten gesloten.
- Alle betrokkenen moeten een aanvraag kunnen doen voor de uitoefening van rechten. Zoals het opvragen, wijzigen, verwijderen van hun gegevens. Met het inrichten van systemen wordt hier rekening mee gehouden, informatie moet makkelijk kunnen worden opgehaald. Betrokkenen moeten hun gegevens makkelijk kunnen krijgen (in een gewenst format) en doorgeven aan andere instanties.
- Door het DB is mandaat verleend aan de directeur om besluiten ten aanzien van de uitoefening van rechten te nemen.
- Om te voldoen aan de informatieverplichtingen zijn procedures richting de betrokkenen opgesteld, is privacybeleid door het DB vastgesteld en is een privacystatement op de website van de RUD Utrecht geplaatst.

3 Risico

3.1 Risicoanalyse

Verschillende factoren kunnen het beoogde eindresultaat in de weg staan. De belangrijkste twee zijn het ontbreken van draagvlak en het ontbreken van budget en menskracht om de benodigde passende beveiligingsmaatregelen te treffen.

Daarnaast kan een gebrek aan tijd worden genoemd als bedreiging en het laten prevaleren van klantvriendelijkheid en toegankelijkheid tot informatie boven de bescherming van persoonsgegevens.

De Autoriteit Persoonsgegevens kan zeer hoge boetes opleggen voor het niet op 25 mei 2018 voldoen aan de AVG.

Om de bovengenoemde risico's te voorkomen dient het belang van een juiste implementatie van de AVG voor het MT, de projectgroep en alle medewerkers duidelijk te zijn. Bewustzijn, draagvlak en menskracht zijn vereisten voor het laten slagen van het project.

3.2 Communicatie

Communicatie is een belangrijk onderdeel voor een succesvolle implementatie van de AVG. Alle medewerkers en het management dienen privacybewust te zijn.

De communicatiemedewerkers dienen ook betrokken te worden aangezien de website aangepast moet worden. Voor een ieder moet duidelijk worden hoe de RUD Utrecht met persoonsgegevens omgaat (een privacy statement). Tevens moet worden vermeld hoe betrokkenen hun rechten kunnen uitoefenen.

Het is zinvol de opdrachtgevers, voor wie de RUD Utrecht taken in mandaat uitvoert en als uitvloeisel daarvan persoonsgegevens verwerkt, te informeren over het project en de getroffen maatregelen om te voldoen aan de AVG.

3.3 Middelen

Een inschatting van het aantal uren dat benodigd is per deelnemer is lastig te maken. Wellicht is op sommige momenten extra inspanning nodig van medewerkers, bijvoorbeeld om inzicht te krijgen in alle verwerkingen die plaatsvinden binnen de RUD Utrecht.
De inzet om de AVG gerelateerde maatregelen te implementeren zal gedragen worden door een doorsnede van de organisatie:

- Bedrijfsvoering algemeen: IV Manager (Mike Barten), IT Security specialist (Dennis Baaten) en medewerker Kwaliteit (Betsie Panjer)
- Bedrijfsvoering specifiek: proces manager, functioneel beheerders, HRM, Communicatie, Jurist, medewerker TOPP
- Per team inzet van medewerkers met inhoudelijke kennis over datastromen en benodigde/te gebruiken informatie

De hieronder genoemde uren zijn gemiddelden;

Gerelateerde inzet in uren en kosten laat het volgende beeld zien:

	Uren/week	# Weken	Totaal uren	Totaal kosten in €	
Projectleider	2	16	32	2880,-	Reguliere functie IV Manager
Security specialist	2	16	32	2880,-	Reguliere functie Security consultant
Projectmedewerker	24	16	344	0,-	Reguliere functie medewerker Kwaliteit
Jurist	4	10	40	2600,-	
Procesmanager	2	8	16	0,-	Reguliere functie Procesmanager
Functioneel beheer	2	8	16	0,-	Reguliere functie functioneel beheerders
					Reguliere functie
HRM	2	10	20	0,-	HRM
Communicatie	2	4	8	0,-	Reguliere functie communicatie medewerkers
Medewerker TOPP	4	16	64	4160,-	
Inzet teams	10	4	40	2600,-	

Er wordt uitgegaan van 65 euro interne kosten per uur per medewerker

De dekking van deze kosten wordt als volgt gevonden:
Medewerkers waar staat verwoord reguliere functie worden geacht budget neutraal (vanuit hun organieke rol) de inzet te geven voor het project. De inzet van de jurist, Medewerker TOPP en de medewerkers uit de teams vinden dekking voor hun inzet in het door het Bestuur extra beschikbaar gestelde budget.

3.4 Tijdlijn en prioritering

Omdat de tijd tot 25 mei beperkt is en de RUD Utrecht nog een betrekkelijk nieuwe organisatie is, die nog volop is ontwikkeling is, zal per 25 mei 2018 de minimale ambitie zijn verwezenlijkt. In de periode na 25 mei 2018 zal een verdere doorontwikkeling op het onderwerp plaatsvinden. Daarom is onderstaande prioritering aangebracht in de acties die in ieder geval uitgevoerd moeten zijn. In de bijlage zijn alle acties benoemd en daarin is aangegeven welke acties op een later tijdstip zullen worden uitgevoerd.

1.	Vaststellen Privacybeleid en implementatieplan MT	februari 2018
2.	Vaststellen Privacybeleid DB/AB	maart 2018
3.	Keuze FG in/uit huis en opstarten sollicitatie	februari 2018
4.	Maken en vaststellen procedure en register datalekken	februari 2018
5.	Opstellen verwerkingsregister	jan/mrt 2018
6.	Bewustmaking medewerkers	mrt/juni 2018
7.	Afsluiten verwerkingsovereenkomsten partners/leveranciers	mrt/juni 2018
8.	Benoeming FG	april 2018
9.	Privacystatement op website	mrt. 2018

Bijlage 1: Actielijst uit het Privacybeleid

Deze bijlage beschrijft per eis uit het privacybeleid de relevante acties. Alleen de acties die horen bij de prioriteiten in 3.4 zijn nader uitgewerkt. Overige acties die op een later tijdstip zullen worden uitgevoerd, zijn grijs gemaakt.

Eis uit privacybeleid: opzetten verwerkingsregister. Doel en context van de verwerking worden binnen de RUD Utrecht enerzijds vastgelegd in een verwerkingsregister en anderzijds in overeenkomsten met verwerkers. Let op: ook de eigen verwerkingen dienen te worden vastgelegd in het verwerkingsregister.

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

Actie 1: Definiëren wat er per verwerking vastgelegd dient te worden (template verwerkingsregister).
- Uitvoerder: Betsie
- Benodigde tijd: 4 uur
- Datum start: 1-1-2018
- Datum klaar: 1-3-2018

Actie 2: Uitvraagformulier (meerkeuze) t.b.v. inventarisatie opstellen.
- Uitvoerder: Betsie
- Benodigde tijd: 8 uur
- Datum start: 1-1-2018
- Datum klaar: 1-3-2018

Actie 3: Invullen uitvraagformulier t.b.v. inventarisatie
- Uitvoerder: ongeveer 10 personen in organisatie
- Benodigde tijd: 4 uur per persoon. Totaal 40 uur.
- Datum start: 1-1-2018
- Datum klaar: 1-3-2018

Actie 4: Verwerken van ingevulde uitvraagformulieren (inventariseren / vullen van register).
- Uitvoerder: Betsie
- Benodigde tijd: 8 uur
- Datum start: 1-1-2018
- Datum klaar: 1-3-2018

Actie 5: Controle volledigheid verwerkingsregister en aanvullen van open plekken (vullen / inventariseren).
- Uitvoerder: Betsie + jurist
- Benodigde tijd: 20 uur + 8 uur
- Datum start: 1-1-2018
- Datum klaar: 1-3-2018

Actie 6: Borgen up-to-date houden van verwerkingsregister.
- Uitvoerder: Betsie
- Benodigde tijd: 20 uur
- Datum start: n.n.t.b. (na 25-5-2018)
- Datum klaar: n.n.t.b.

Eis privacybeleid: *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 mate waarin burgers hun privacy geborgd weten, wordt in belangrijke mate bepaald door de kwaliteit en de professionaliteit van de medewerkers, ook met betrekking tot privacy en gegevensverwerking. Dat betekent dat het belangrijk is dat privacy, zorgvuldige omgang met gegevens en triage ten aanzien van noodzakelijke gegevens, onderdeel moeten zijn va de professionele bagage van de medewerkers. Ook zullen teamleiders actief moeten sturen op een zorgvuldige omgang met gegevens en zorgen dat wordt gewerkt conform het privacy beleid.

Eis uit privacybeleid: *De RUD Utrecht publiceert een privacybeleid/statement op de website waarin staat beschreven tot wie personen zich kunnen wenden voor vragen.*

Actie 1: Opstellen privacystatement website.
- Uitvoerder: Dennis
- Benodigde tijd: 8 uur
- Datum start: 1-1-2018
- Datum klaar: 1-5-2018

Actie 2: Initiële bewustwording privacy.
- Uitvoerder: Dennis
- Benodigde tijd: 16 uur
- Datum start: 1-1-2018
- Datum klaar: 1-5-2018

Actie 3: Trainingen op basis van de ontstane behoeften.
- Uitvoerder: Medewerker communicatie/HRM/privacy officer
- Benodigde tijd: 40 uur
- Datum start: n.n.t.b. (na 25-5-2018)
- Datum klaar: n.n.t.b.

Actie 4: Opstellen gedragscode medewerkers.
- Uitvoerder: communicatiemedew. en privacy officer
- Benodigde tijd: 24 uur
- Datum start: n.n.t.b. (na 25-5-2018)
- Datum klaar: n.n.t.b.

Eis uit privacybeleid: *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:*

Actie 1: Maken procedures voor inzage, muteren en verwijderen van gegevens
- Uitvoerder: Betsie, medewerker procedures.
- Benodigde tijd: 12 uur
- Datum start: n.n.t.b. (na 25-5-2018)
- Datum klaar: n.n.t.b.

Actie 2: Maken procedure voor overdragen van gegevens
- Uitvoerder: Betsie, medewerkersprocedures
- Benodigde tijd: 12 uur
- Datum start: n.n.t.b. (na 25-5-2018)
- Datum klaar: n.n.t.b.

Eis uit privacybeleid: *De RUD Utrecht beschikt over een procedure voor het melden van datalekken.*

Actie 1: Maken procedure voor het melden van datalekken
- Uitvoerder: Dennis
- Benodigde tijd: 16 uur
- Datum start: 1-1-2018
- Datum klaar: 1-3-2018

Actie 2: Maken inbreukenregister waarin alle inbreuken (waaronder ook datalekken) worden gedocumenteerd
- Uitvoerder: Betsie
- Benodigde tijd: 8 uur
- Datum start: n.n.t.b. (na 25-5-2018)
- Datum klaar: n.n.t.b.

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

Actie 1: uitzoeken of we deze middelen hebben
- Uitvoerder: Dennis, ICT Houten
- Benodigde tijd: n.n.t.b.
- Datum start: n.n.t.b. (na 25-5-2018)
- Datum klaar: n.n.t.b.

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

Actie 1: opstellen informatiebeveiligingsbeleid en baseline
- Uitvoerder: Dennis
- Benodigde tijd: n.n.t.b. (ander traject)
- Datum start: n.n.t.b. (na 25-5-2018)
- Datum klaar: n.n.t.b.

Eis uit privacybeleid: *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.*

Eis uit privacybeleid: *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.*

Actie 1: Opstellen classificatiemodel t.b.v DPIA
- Uitvoerder: n.n.t.b.
- Benodigde tijd: n.n.t.b.

- Datum start: n.n.t.b. (na 25-5-2018)
- Datum klaar: n.n.t.b.

Actie 2: Opstellen procedure voor uitvoeren van DPIA (wanneer wel, wanneer niet, en hoe)
- Uitvoerder: n.n.t.b.
- Benodigde tijd: n.n.t.b.
- Datum start: n.n.t.b. (na 25-5-2018)
- Datum klaar: n.n.t.b.

Eis uit privacybeleid: *De RUD Utrecht borgt privacy-by-design en privacy-by-default 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.*

Actie 1: Verankeren van aandacht voor privacy in bestaande processen en procedures
- Uitvoerder: n.n.t.b.
- Benodigde tijd: n.n.t.b.
- Datum start: n.n.t.b. (na 25-5-2018)
- Datum klaar: n.n.t.b.

Eis uit privacybeleid: *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.*

Eis uit privacybeleid: *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.*

Actie 1: opstellen procedure anonimiseren
- Uitvoerder: n.n.t.b.
- Benodigde tijd: n.n.t.b.
- Datum start: n.n.t.b. (na 25-5-2018)
- Datum klaar: n.n.t.b.

Eis uit privacybeleid: *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.*

Eis uit privacybeleid: *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.*

Actie 1: opstellen procedure encryptie
- Uitvoerder: n.n.t.b.
- Benodigde tijd: n.n.t.b.
- Datum start: n.n.t.b. (na 25-5-2018)
- Datum klaar: n.n.t.b.

Eis uit privacybeleid: *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.*

Eis uit privacybeleid: *RUD Utrecht past bestaande overeenkomsten aan, zodat deze voldoen de AVG vereisten.*

Eis uit privacybeleid: *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 optreedt als verwerkingsverantwoordelijke.*

Eis uit privacybeleid: *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.*

Actie 1: Overzicht maken welke verwerkingsovereenkomsten en zijn en welke missen (o.b.v. verwerkingsregister).
- Uitvoerder: privacy officer, contract beheer
- Benodigde tijd: 20 uur
- Datum start: 1-2-2018
- Datum klaar: 25-5-2018

Actie 2: Bestaande contracten en overeenkomsten controleren of ze voldoen.
- Uitvoerder: jurist, privacy officer
- Benodigde tijd: 40 uur
- Datum start: 1-2-2018
- Datum klaar: 25-5-2018

Actie 3: verwerkingsovereenkomst controleren of deze voldoet aan de AVG
- Uitvoerder: Jurist, privacy officer
- Benodigde tijd: 8 uur
- Datum start: 1-2-2018
- Datum klaar: 15-2-2018

Actie 4: verwerkings/bewerkingsovereenkomsten afsluiten met opdrachtgevers en leveranciers.
- Uitvoerder: Verantwoordelijke contract
- Benodigde tijd: 40 uur
- Datum start: 1-2-2018
- Datum klaar: 25-5-2018

Eis uit privacybeleid: *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.*

Actie 1: Keus MT RUD of zij deze medewerker zelf in huis wil hebben of dat ze deze inhuurt.

- Uitvoerder: Betsie
- Benodigde tijd: 8 uur
- Datum start: 1-1-2018
- Datum klaar: 15-2-2018

Actie 2: indien de RUD deze FG zelf wil dan dient een profiel en functiebeschrijving te worden opgesteld.

- Uitvoerder: HRM
- Benodigde tijd: 8 uur
- Datum start: 1-1-2018
- Datum klaar: 15-2-2018

Actie 3: Ingeval van actie 2 dient (interne)werving en selectieprocedure te worden gestart.

- Uitvoerder: HRM
- Benodigde tijd: 12 uur
- Datum start: 15-2-2018
- Datum klaar: 25-5-2018

Actie 4: indien de RUD er voor kiest niet zelf een FG in dienst te hebben dan procedure starten voor externe inhuur van FG

- Uitvoerder: HRM
- Benodigde tijd: 8 uur
- Datum start: 15-2-2018
- Datum klaar: 25-5-2018

Actie 5: Benoemen en laten registreren FG bij AP.

- Uitvoerder: DB, HRM
- Benodigde tijd: 4 uur
- Datum start: 1-1-2018
- Datum klaar: 25-5-2018

Actie 6: Bevoegdheden, positionering, middelen FG vastleggen in protocol.

- Uitvoerder: MT, HRM, OR
- Benodigde tijd: 14 uur
- Datum start: 1-1-2018
- Datum klaar: 25-5-2018

Eis uit privacybeleid: *De RUD Utrecht dient te borgen dat wanneer zij persoonsgegevens laat verwerken door organisaties buiten Europa:*
a) *dat er een Europees modelcontract is afgesloten, of*
b) *in het geval van Amerikaanse bedrijven, dat deze bedrijven zijn opgenomen in het EU-U.S. Privacy Shield.*

Eis uit privacybeleid: *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.*

Actie 1: Besluit nemen omtrent het gebruik van niet-Europese leveranciers

- Uitvoerder: n.n.t.b.
- Benodigde tijd: n.n.t.b.
- Datum start: n.n.t.b. (na 25-5-2018)
- Datum klaar: n.n.t.b.

Eis uit privacybeleid: *De RUD Utrecht handelt haar zaken af met de Autoriteit Persoonsgegevens in Nederland.*

Geen actie vereist