Jaarrapportage bescherming persoonsgegevens RUG 2018

De privacymanagementorganisatie in de steigers

Mr. A.R. Deenen
Functionaris voor de Gegevensbescherming

28 februari 2019

Managementsamenvatting en conclusie

In lijn met het Algemeen Beleid Bescherming Persoonsgegevens Rijksuniversiteit Groningen doet de Functionaris voor de Gegevensbescherming (“FG”) verslag van de staat van de privacymanagementorganisatie en de bescherming van persoonsgegevens bij de Rijksuniversiteit Groningen (“RUG”) over 2018. Dit wordt in tien onderwerpen uiteengezet met het bijbehorende volwassenheidsniveau per onderwerp.

Hoofdstuk 3 (“H.3”) Privacybeleid en inbedding in de organisatie:

het RUG-brede privacybeleid is opgesteld en centraal vastgesteld. Het implementeren ervan en het toezichthouden op de naleving van het beleid zijn de volgende doelen voor de RUG.

H.4 Risicomanagement:

op (de)centraal niveau dienen privacyrisico’s te worden vastgesteld. Het mitigeren van deze risico’s zal als RUG-breed plan moeten worden vastgesteld en uitgevoerd.

H.5 Doelbinding en intern toezicht:

bij de RUG ontbreekt er op dit moment een eenduidige controle op de rechtmatigheid en de doelen van alle bestaande en nieuwe verwerkingen van persoonsgegevens. Voor het interne toezicht is de FG aangesteld. In 2018 schoof zijn rol van kwartiermaker naar toezichthouder. Structurele ondersteuning van de FG is noodzakelijk wil hij zijn wettelijke taken kunnen uitvoeren.

H.6 Register:

het register geeft inzicht en overzicht van de verwerkingen van persoonsgegevens. De RUG hanteert de Research Data Management Plan-tool om alle verwerkingen in kaart te brengen. Richtlijnen voor de invulling en het beheer van het register zijn in ontwikkeling, maar nog niet formeel op centraal niveau vastgesteld.

H.7 Kwaliteitsmanagement:

het niveau van kwaliteitsmanagement binnen de RUG is sterk afhankelijk van de categorie betrokkene en de plaats binnen de organisatie. Met name de levenscyclus van studentgegevens en gegevens over onderzoekssubjecten vraagt aandacht. Hier valt nog veel “winst” te behalen.

H.8 Bewaren van persoonsgegevens:

in het project Digitaal Student Dossier wordt gestreefd naar een uniforme organisatiebrede wijze om de bewaartermijnen vast te stellen en toe te passen. Voor gegevens van medewerkers gaat Best Practice 2020 een uitkomst bieden, waarbij het opstellen van ‘best practices’ en een duidelijke verdeling van verantwoordelijkheden cruciaal is.

H.9 Beveiligen van persoonsgegevens:

tot op heden zijn de beveiligingsrisico’s niet structureel in beeld gebracht. De risico’s en mitigerende maatregelen worden enkel op informeel niveau en naar keuze van de interne verantwoordelijke vastgesteld. Tevens zijn richtlijnen voor de verwerkingen op de werkvloer vereist en dient er scherp te worden gekeken naar de beveiliging bij verwerkers (derde partijen).

H.10 Informatieverstrekking en rechten betrokkenen:

de RUG kent een algemene privacyverklaring, deze informeert de studenten en medewerkers over de omgang met persoonsgegevens. Veel verwerkingen op het laagste abstractieniveau zijn nog niet transparant (gemaakt) voor de betrokkenen. Ook onderzoekers hebben ondersteuning nodig bij de informatieverstrekking aan onderzoekssubjecten.

H.11 Verwerkersovereenkomsten en doorgifte:

de RUG heeft met een beperkte groep van verwerkers afspraken gemaakt. In kaart brengen van de missende verwerkers-overeenkomsten is de eerste stap. Daarnaast zijn richtlijnen omtrent doorgifte gewenst, omdat verwerkingen buiten de EU (lees: EER) met extra waarborgen moeten zijn omkleed.

H.12 Datalekken:

de RUG heeft meerdere datalekken gemeld. Een datalekken-protocol is aanwezig en wordt nageleefd. Het interne meldpunt voor het melden van datalekken mag meer attentie krijgen bij studenten en medewerkers, onderzoekers daarbij in het bijzonder.

H.13 Conclusie:

de RUG is gestart met de opzet van de privacymanagementorganisatie. De RUG bevindt zich op het volwassenheidsniveau 1,3 op een schaal van 0-5.
Aan de hand van de interne werkplannen en dit jaarrapport heeft de RUG afdoende handvatten om de borging van privacy verder te laten groeien.
Een ambitieus, maar realistisch streven voor de RUG zou zijn om in 2020 op het volwassenheidsniveau 2,0 te zitten. De volgende stappen geven beknopt weer wat hiervoor noodzakelijk is.

1. RUG-breed

- De RUG dient een start te maken met de implementatie van de beschreven PDCA-cyclus uit het privacybeleid.
- De RUG moet streven om organisatiebreed naar een eenduidig en formeel vastgestelde toepassing van de AVG te gaan, hiervoor kan een Privacy Baseline worden opgezet.
- Een risicomanagementaanpak moet worden vastgesteld en toegepast waarbij de privacyrisico's op een (de)centraal niveau in kaart moeten worden gebracht.
- De privacybeginselen uit de AVG dienen in de gehele organisatie op een uniforme wijze te worden ingebed.
- Processen dienen te worden gestandaardiseerd en vormen de basis van een functioneel register. Aan deze gestandaardiseerde processen worden de instellingsbrede doelen, bewaartermijnen en beveiligingsmaatregelen gekoppeld.
- Er dienen richtlijnen rondom de veilige verzending van (bijzondere) persoonsgegevens te worden vastgesteld.
- Het Centraal Loket Privacy dient toegankelijk(er) te zijn voor betrokkenen.

2. Specifiek domein Bedrijfsvoering

- Nieuwe werknemers dienen de AVG-cursus te volgen om zorg te dragen voor een basisniveau aan kennis bij medewerkers.
- Medewerkers met een bijzondere taak, waaronder de leden van ethische commissies, dienen opgeleid te worden in de aspecten van privacy in onderzoek.
- 'Best practices' dienen te worden opgesteld rond de verwerking van de persoonsgegevens van medewerkers. Deze zijn cruciaal bij de toepassing van AFAS.
- De FG en de privacysectie van ABJZ dienen structureel ondersteund te worden.

3. Specifiek domein Onderwijs

- Ten behoeve van de zorgvuldige verwerking van studentgegevens dienen uitkomsten van het Project DSD te worden geïmplementeerd in de onderwijsprocessen.
- De RUG dient DPIA's uit te voeren binnen SIA op de verwerking van persoonsgegevens van (aankomende) studenten.
- De meest omvangrijke en risicovolle verwerkingen binnen de RUG dienen inzichtelijk te worden gemaakt (bijvoorbeeld middels privacyverklaringen).

4. Specifiek domein Onderzoek

- Aankomend jaar dienen de diensten en producten uit het programma HSR geïmplementeerd te worden. Hieronder valt ook het opnemen van de handleiding "Starting with a DPIA methodology for human subject research" in de voorbereiding van onderzoek met persoonsgegevens.
- De RUG dient technische en organisatorische ondersteuning te bieden voor het pseudonimiseren en anonimiseren van persoonsgegevens in onderzoek.
- De RUG dient te beginnen met het creëren van bewustwording onder de onderzoekers over (het melden van) datalekken.

Inhoudsopgave

1. Voorwoord 1
2. Inleiding 2
3. Privacybeleid en inbedding in de organisatie 3
4. Risicomanagement 6
5. Doelbinding en intern toezicht 9
6. Register 12
7. Kwaliteitsmanagement 15
8. Bewaren van persoonsgegevens 18
9. Beveiligen van persoonsgegevens 20
10. Informatieverstrekking en rechten betrokkenen 25
11. Verwerkersovereenkomsten en doorgifte 28
12. Datalekken 30
13. Conclusie 33
Bijlage 1. Privacy Volwassenheidsmodel CIP 34

Verklarende woordenlijst

Autoriteit Persoonsgegevens – de Nederlandse toezichthouder met betrekking tot de bescherming van persoonsgegevens;

AVG – Algemene Verordening Gegevensbescherming (de officiële Engelstalige benaming: GDPR) ;

Betrokkene – de natuurlijke persoon waarop de persoonsgegevens betrekking hebben;

Bijzondere persoonsgegevens – persoonsgegevens die gevoelig(er) van aard zijn en daarom beter beveiligd (bijvoorbeeld gegevens over geaardheid, strafrechtelijk verleden en gezondheid);

Datalek – inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of toegang tot persoonsgegevens;

DPIA – een Data protection impact assessment (in het Nederlands: Gegevensbeschermingseffectbeoordeling) is een inventarisatie van risico's en maatregelen;

Europese privacyverordening – *zie AVG;*

FG – de Functionaris voor de gegevensbescherming is de onafhankelijke interne toezichthouder;

GDPR – General Data Protection Regulation (Regulation (EU) 2016/679);

Ontvanger – een natuurlijke persoon of organisatie waaraan persoonsgegevens worden verstrekt;

Persoonsgegevens – alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (*zie ook Betrokkene)*;

Privacybeleid – Algemeen Beleid Bescherming Persoonsgegevens Rijksuniversiteit Groningen;

Privacyverklaring – Algemene privacyverklaring Rijksuniversiteit Groningen;

Pseudonimiseren – een dataset omvormen zodat data niet direct te herleiden valt tot personen;

Register – een verplicht overzicht met de verwerkingen van persoonsgegevens;

UAVG – Uitvoeringswet Algemene verordening gegevensbescherming;

Verantwoordelijke – een natuurlijke persoon of organisatie die het doel en de middelen van de verwerking van persoonsgegevens vaststelt (binnen dit jaarrapport is dat de RUG);

Verwerker – een natuurlijke persoon of organisatie die ten behoeve van de Verantwoordelijke persoonsgegevens verwerkt;

Verwerkersovereenkomst – overeenkomst tussen de Verantwoordelijke en Verwerker over de wijze waarop persoonsgegevens worden verwerkt en beveiligd;

Verwerking – een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens (zoals verzamelen, ordenen, opslaan, opvragen, gebruiken, verspreiden en verwijderen);

Verwerkingsverantwoordelijke – *zie Verantwoordelijke.*

1. Voorwoord

Voor u ligt de Jaarrapportage Bescherming Persoonsgegevens RUG 2018 (“jaarrapport”) voor het College van Bestuur van de RUG. Het jaarrapport is geschreven door de Functionaris voor de Gegevensbescherming (“FG”) van de RUG.

Het jaarrapport is informerend, signalerend en adviserend van aard. Dit komt overeen met de wettelijke invulling[1] van de FG en de taken in het Algemeen Beleid Bescherming Persoonsgegevens Rijksuniversiteit Groningen (“privacybeleid”).

In het jaarrapport worden de aspecten met het hoogste risico benoemd en de daarbij voorgestelde maatregelen. Ondanks haar omvang is het jaarrapport niet uitputtend bedoeld. Wel is het jaarrapport goed te gebruiken als naslagwerk gedurende 2019.

Verder bevat het jaarrapport terminologie uit de Europese privacywetgeving en interne (beleids)stukken. De verklarende woordenlijst voorin het jaarrapport licht de veelgebruikte (juridische) terminologie toe.

[1] De taken van de Functionaris voor de Gegevensbescherming zijn beschreven in art. 39 AVG.

2. Inleiding

25 mei 2018 is de Algemene Verordening Gegevensbescherming ("AVG") van toepassing verklaard in de Europese Unie. Met genoeg aandacht in de media voor de (mogelijke) gevolgen werd Nederland wakker. De RUG was bekend met de voorgaande wetgeving en handelde daar als verantwoordelijke in zekere mate reeds naar.

De AVG stelt nieuwe eisen aan de omgang met persoonsgegevens ten opzichte van de Wet bescherming persoonsgegevens ("Wbp"). Waar de rechten van de betrokkenen beperkt worden uitgebreid, dient de RUG wel aan een aantal nieuwe verplichtingen te voldoen. Deze nieuwe verplichtingen zien met name op de verantwoordingsplicht. Denk hierbij aan het inrichten van het register van verwerkingen, het uitvoeren van *data protection impact assessments*[2] ("DPIA"). Ook het sluiten van verwerkersovereenkomsten met derden valt hieronder, maar was reeds verplicht onder de Wbp.

Sinds het vierde kwartaal van 2016 is de RUG gestart met het zogenaamde Project Compliance AVG. Nu twee jaar later schetst de FG een beeld van de wijze waarop de privacymanagementorganisatie binnen de RUG is ingericht en hoe deze functioneert.

Bij het vaststellen van voorgaande is het volwassenheidsmodel gehanteerd zoals deze door het Centrum Informatiebeveiliging en Privacybescherming is vastgesteld.[3] Een volwassenheidsmodel geeft inzicht in het niveau (0 tot 5) waarop een organisatie zich bevindt.

Zoals zal blijken uit dit jaarrapport zijn veel "privacyprocessen" en de inrichting daarvan onlosmakelijk verbonden met reguliere bedrijfsprocessen. Een gebrek in de privacymanagementorganisatie is derhalve vaak te herleiden tot gebrekkige (controle op) reguliere bedrijfsprocessen. Dit betekent omgekeerd dat het verbeteren van de privacymanagement ook positieve gevolgen kan hebben voor de reguliere bedrijfsvoering.

Op basis van haar privacymissie en -visie streeft de RUG minimaal het volwassenheidsniveau **3** na. Elk niveau lager duidt in beginsel op een tekortkoming in compliance met de AVG.

Op het moment van schrijven van dit jaarrapport is middels een assessment het algemene volwassenheidsniveau van de RUG vastgesteld op **1,3**. Dit is een mooi resultaat gezien de inspanningen van het afgelopen jaar.

Het algemene volwassenheidsniveau is verdeeld in tien onderdelen; beschreven in tien hoofdstukken. Per onderdeel zal het huidige volwassenheidsniveau getoond worden. Dit wordt weergegeven middels de gekleurde balk zoals hierboven is geplaatst. Als laatste beschrijft dit jaarrapport per onderdeel de algemene risico's ( ), de specifieke risico's voor de RUG ( ) en de stappen om als RUG tot een hoger niveau te komen ( ).

---

[2] De Autoriteit Persoonsgegevens beschrijft de DPIA als "[..] een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En om daarna maatregelen te kunnen nemen om de risico's te verkleinen."
[3] M. Koers e.a. (red), 'Privacy Volwassenheidsmodel', *Centrum voor Informatiebeveiliging en Privacybescherming* 2 november 2017, versie 3.0.9, cip-overheid.nl. Zie ook Bijlage 1. Privacy Volwassenheidsmodel CIP.

3. Privacybeleid en inbedding in de organisatie

Met het privacybeleid geeft de RUG aan op welke manier zij voldoet aan de geldende wet- en regelgeving. Wet- en regelgeving zijn externe factoren, dus periodieke beoordeling is vereist om te kijken of het staande beleid nog volstaat. Ook interne factoren als wijziging van missie en visie, maar ook (in)effectiviteit van het beleid zijn redenen om periodiek te evalueren. Het beleidsproces cyclisch inrichten is derhalve een vereiste.

Het College van Bestuur ("CvB") heeft in 2018 het Algemeen Beleid Bescherming Persoonsgegevens ("privacybeleid") vastgesteld. Hierin zijn tevens de missie en visie uiteengezet voor wat betreft de bescherming van persoonsgegevens.

Het volwassenheidsniveau op dit onderdeel binnen de RUG:

Algemene risico's

Indien privacybeleid en/of transparante taakverdeling ontbreekt, ontstaat er onduidelijkheid over hetgeen wordt verwacht van een organisatie. Dit vergroot op zijn beurt de kans dat persoonsgegevens in strijd met wet- en regelgeving worden verwerkt en het privacybeleid en relevante wet- en regelgeving ineffectief worden geïmplementeerd.

PDCA-cyclus

Om het privacybeleid te borgen, zal de RUG dienen te starten met de implementatie van de beschreven PDCA-cyclus. Hierbij zal aandacht moeten worden geschonken aan de verdeling van taken en verantwoordelijkheden. Ook zal bij de implementatie van de PDCA-cyclus, afstemming gezocht moeten worden met de PDCA-cyclus voor de informatiebeveiliging. Het privacybeleid vraagt namelijk ook om de toepassing van (technische) beveiligingsmaatregelen.

Verder zal het streven van de RUG moeten zijn om de planning van de benodigde middelen te koppelen aan het privacybeleid. Een eerste aanzet daartoe wordt centraal en decentraal in 2019 gedaan met het opstellen van de werkplannen.

Daarnaast dient de RUG te beginnen bij het begin; de zogenaamde privacybeginselen[4] uit de AVG dienen in de gehele organisatie op een uniforme wijze te worden ingebed.

[4] De privacybeginselen worden gevonden in artikel 5 AVG.

Een uniforme wijze ontbreekt nu. De toepassing hiervan wordt momenteel op verwerkingsniveau informeel bepaald.

Inzet (faculteits)besturen en directies

Om het privacybeleid te borgen zal een correcte en tijdige implementatie van de PDCA-cyclus op centraal en decentraal niveau benodigd zijn. Hiervoor is de inzet en betrokkenheid van de faculteitsbesturen en directies onontbeerlijk.

In het afgelopen jaar zijn binnen alle faculteiten en diensten privacy- en securitycoördinatoren aangewezen. Deze coördinatoren zijn verantwoordelijk voor de inventarisatie van alle verwerkingen binnen de eigen faculteit/dienst, maar ook voor het initiëren van DPIA's en beantwoording van vragen over privacy en security van collega's.

De coördinatoren zijn bij alle faculteiten en diensten aangewezen, maar misten tot ruim in 2018 in veel gevallen de bestuurlijke ondersteuning in de vorm van tijd/geld. Dit uitte zich in een gebrekkige inventarisatie van de processen binnen de faculteiten/diensten.

Met de verdere inbedding van het privacybeleid en daarmee de verplichting om een werkplan aan te leveren is het beeld de laatste vier maanden aanzienlijk gewijzigd. Het merendeel van de faculteiten en diensten heeft op dit moment een of meerdere coördinatoren aangewezen die gefaciliteerd word(t)(en) door het faculteitsbestuur of directie. Dit is één van de belangrijkste vereisten om als RUG te komen tot een hoger volwassenheidsniveau en daarmee tot compliance met de AVG.

Naast de decentrale besturen dient ook het College van Bestuur zijn bijdrage leveren. Het CvB kan allereerst het belang van de implementatie van de privacyorganisatie onderschrijven bij de Bestuurlijke Overleggen met de eenheden. Daarnaast kan het CvB haar beleidsmedewerkers vragen middels "Privacy by Design" te werken wanneer het de verwerking van persoonsgegevens aangaat.[5]

Risico bij de implementatie van de AVG

Een risico bij de implementatie van een privacymanagementorganisatie is dat er bij de RUG "rule driven" gewerkt gaat worden. Dit betekent dat de RUG de verwerking van persoonsgegevens in detail gaat voorschrijven. In dat geval zullen medewerkers zich meer passief opstellen. Een dergelijke werkwijze past niet bij de aard van de organisatie. Werknemers en studenten moeten hun eigen verantwoordelijkheid (kunnen) nemen. De RUG dient wel de kaders te stellen om deze werkwijze in goede banen te leiden.

De kaders vindt de RUG in de zogenaamde privacybeginselen. Hierbij kan gedacht worden aan "dataminimalisatie"[6], "doelbinding"[7], "opslagbeperking"[8] en "transparantie".

[5] Privacy by Design is vastgelegd in art. 25 AVG en vraagt van de Verantwoordelijke om bij het ontwerp en inrichting van verwerkingen rekening te houden met de risico's voor de rechten en vrijheden van de natuurlijke personen.
[6] Niet meer persoonsgegevens verwerken dan noodzakelijk voor het doel van de verwerking.
[7] Meer over doelbinding in Hoofdstuk 5. Doelbinding en intern toezicht.
[8] Opslagbeperking en bewaartermijnen komen aan bod in Hoofdstuk 8. Bewaren van persoonsgegevens.

Het streven zal zijn om organisatiebreed naar een eenduidig en formeel vastgestelde toepassing te gaan. Hiervoor roept de RUG een Privacy Baseline in het leven of stelt een toegankelijke richtlijn op.

Kennis personeel

Verwerking van persoonsgegevens vindt plaats op de werkvloer. Zorgvuldige omgang met persoonsgegevens begint derhalve bij de circa 6.000 medewerkers bij de RUG.

Het is ondoenlijk en onwenselijk om van alle medewerkers privacyprofessionals te maken. Desalniettemin is het belangrijk om de medewerkers die persoonsgegevens verwerken (praktisch eenieder) kennis bij te brengen over de privacybeginselen uit de AVG. Het gaat in dat geval om de gedachte achter de AVG en niet om de letterlijke wettekst.

De RUG kent reeds een (interne) Workshop AVG die door meer dan 400 medewerkers is gevolgd bij het CIT of op locatie. Om zorg te dragen voor een basisniveau aan kennis bij medewerkers, wordt geadviseerd om nieuwe medewerkers bij indiensttreding standaard de Workshop AVG te laten volgen.

Kennis ondersteunend personeel onderzoek

Medewerkers met taken die meer specifieke kennis vereisen van de AVG, krijgen momenteel al een cursus op maat. Hieronder vallen onder meer de medewerkers betrokken bij (Europese) aanbestedingen. Hetzelfde is ook vereist voor de ethische commissies.

De European Data Protection Board[9] schrijft in haar adviezen dat met wetenschappelijk onderzoek wordt bedoeld onderzoek dat in lijn is met sector-gebonden richtlijnen en ethische normen.[10] Daarnaast worden de ethische commissies gemeld in de Nederlandse gedragscode wetenschappelijke integriteit (“Gedragscode WI”) als adviseurs bij de inzet en omgang met onderzoekssubjecten.

Ethiek en privacy zijn bij onderzoek derhalve verweven. Echter is de toestemming voor de ethische aspecten van onderzoek niet hetzelfde als toestemming voor het gebruik van persoonsgegevens binnen onderzoek. Dergelijke kennis is bij menig lid van de ethische commissie nog niet aanwezig.

Het opleiden van medewerkers met een bijzondere taak is niet structureel ingericht, maar is wel aanbevelenswaardig indien deze medewerkers onderzoekers, derden en andere medewerkers moeten adviseren over de juiste toepassing van de AVG.

[9] De European Data Protection Board (“EDPB”) is een gezaghebbend orgaan waarin alle nationale toezichthouders uit de EU zijn verenigd en dat adviezen uitbrengt over de uitleg en toepassing van de AVG.
[10] Article 29 Working Party, ‘Guidelines on consent under Regulation 2016/679’, *WP259* rev. 01, Brussel 10 april 2018, p. 27-28.

4. Risicomanagement

De AVG vraagt om een risicogedreven aanpak. Risicomanagement binnen de RUG bestond in 2017 en 2018 uit signalering, beoordeling en behandeling van privacyrisico's op verwerkingsniveau waarbij veelal informeel werd gehandeld. De RUG werkt vaak reactief wanneer het aankomt op risicomanagement op het gebied van de bescherming van persoonsgegevens.

Om te komen tot het gewenste volwassenheidsniveau zal er een risicomanagementaanpak moeten worden vastgesteld en toegepast. Hierbij dienen de privacyrisico's op een (de)centraal niveau te worden vastgesteld. Het mitigeren van deze risico's dient als RUG-breed plan te worden vastgesteld en daarna te worden uitgevoerd.

Binnen de risicomanagementaanpak van de RUG zal het DPIA organisatiebreed moeten worden geïmplementeerd. Een DPIA is een uitermate geschikt middel om risico's in processen te identificeren en te komen tot passende mitigerende maatregelen. Het DPIA is met de komst van de AVG verplicht geworden voor verwerkingen met een hoog risico.[11]

Idealiter zal het DPIA onderdeel uitmaken van het ontwerpen en inrichten van nieuwe verwerkingen en/of wijzigingen in bestaande verwerkingen.

Het volwassenheidsniveau op dit onderdeel binnen de RUG:

Algemene risico's

Zonder de (tijdige) signalering van privacyrisico's kan de organisatie geen passende maatregelen nemen. De verwerking voldoet derhalve niet aan de eisen die de AVG stelt; er ontstaat een grote(re) kans op inbreuken op de beveiliging van persoonsgegevens. Dergelijke inbreuken kunnen betrokkenen schaden.

Gelet op het feit dat de AVG een risicogebaseerde aanpak nastreeft, zullen hieronder de grootste risicogebieden binnen de RUG worden beschreven.

[11] De verplichting om een DPIA uit te voeren wordt gevonden in art. 35 AVG. In de wetgeving wordt een DPIA ook wel "gegevensbeschermingseffectbeoordeling" genoemd.

Studenten Informatie en Administratie (SIA)

Bij de afdeling Studenten Informatie en Administratie (“SIA”) wordt een groot aantal persoonsgegevens verwerkt. Met meer dan 30.000 inschrijvingen per jaar kan de centrale studentadministratie als een grote verwerker van persoonsgegevens binnen de RUG worden geduid. Gezien de omvang van de verwerking van persoonsgegevens mag worden verwacht dat de studentadministratie passende organisatorische en technische maatregelen neemt om het verlies of onrechtmatig gebruik van de persoonsgegevens te voorkomen.

Bij het bevragen van medewerkers en het doornemen van de systemen van SIA is gebleken dat er organisatorisch en technisch nog veel ‘winst’ te behalen valt wat betreft de bescherming van de persoonsgegevens. Zo zijn de rollen en rechten binnen de RUG niet (formeel) beschreven en vastgelegd. Ook zijn de privacybeginselen geen integraal onderdeel van processen binnen SIA; denk hierbij aan dataminimalisatie of opslagbeperking. Daarnaast wordt er gebruik gemaakt van systemen die niet aan alle eisen van beveiliging en bescherming van (persoons) gegevens voldoen.[12]

Gezien de grote aantallen (bijzondere) persoonsgegevens wordt geadviseerd om op korte termijn DPIA’s uit te voeren binnen SIA op de verwerking van persoonsgegevens van (aankomende) studenten. Daarbij moet meer specifiek naar de systemen Progress.NET en OAS gekeken worden.[13] De DPIA’s leiden uiteindelijk tot een aantal concrete technische en organisatorische maatregelen om de bestaande risico’s te beperken en/of weg te nemen. De RUG dient tevens te borgen dat dergelijke maatregelen worden geïmplementeerd.

Human Resources

Naast het grote aantal studenten, verwerkt de RUG van circa 6.000 medewerkers persoonsgegevens. Hieronder vallen veel gevoelige en bijzondere persoonsgegevens, persoonsgegevens die passende bescherming vereisen. Die bescherming is momenteel niet optimaal; de inrichting van huidige systemen zoals PeopleSoft laat te wensen over.[14]

Net als onder het organisatieonderdeel SIA beschreven, zijn privacybeginselen geen integraal onderdeel van de processen bij HR. Enkel op verwerkingsniveau wordt informeel gekeken naar de inrichting van de HR-processen.

In tegenstelling tot SIA wordt er met de komst van Best Practice 2020 (“BP 2020”) middels privacy by design gewerkt aan de inrichting van de processen binnen HR. Voorafgaand aan de aanbesteding heeft er een DPIA plaatsgevonden én de bescherming van

[12] Waaronder Progress.NET, ProgressWWW en Online Application System (“OAS”).
[13] Het DPIA op project EWS (Programma Zonder Wrijven Geen Glans) benoemt acht risico’s binnen Progress.NET.
[14] De rollen en rechten binnen Peoplesoft kunnen niet altijd zo fijnmazig worden ingesteld als vereist.

persoonsgegevens is integraal onderdeel geweest van de uitvraag van BP 2020. Dit zijn positieve ontwikkelingen.

Onderzoek(ers)

Bij de RUG worden duizenden wetenschappelijke onderzoeken uitgevoerd. Bij een deel daarvan worden persoonsgegevens verwerkt.

Om hoeveel onderzoeken met persoonsgegevens het precies gaat, hoe deze onderzoeken worden uitgevoerd en waar het onderzoek plaatsvindt is grotendeels onbekend.[15] Dit een risico voor de RUG; zij kan momenteel niet voldoen aan haar verantwoordingsplicht. Ook kan de RUG niet garanderen dat bij alle onderzoeken passende technische en organisatorische maatregelen worden getroffen.

Veel onderzoekers zijn nog niet bekend met de verplichtingen uit de AVG (en voorgaande privacywetgeving).[16] Indien zij wel bekend zijn met de verplichtingen, is het voor menig onderzoeker lastig om concrete invulling te geven aan de eisen van de AVG. De RUG biedt nog geen kant-en-klare sets aan maatregelen.[17] Ook worden medewerkers binnen de faculteiten onvoldoende geïnformeerd over de mogelijkheden om binnen de kaders van de AVG onderzoek te verrichten.

Om bovenstaande risico's te mitigeren worden de producten en diensten uit het Programma Human Subject Research ("HSR") opgeleverd en ingezet. Deze worden momenteel geïmplementeerd. Er zal aankomend jaar moeten worden toegezien op de daadwerkelijke en effectieve implementatie binnen de RUG. Daarbij wordt de vindbaarheid en bekendheid hiervan voor de onderzoeker cruciaal; hierbij spelen de faculteiten weer een belangrijke rol.

Los van vraagstukken omtrent de implementatie moet worden bezien of de producten en diensten uit HSR de (privacygerelateerde) vraagstukken van de onderzoekers in de breedte beantwoorden.

[15] Meer hierover in Hoofdstuk 6. Register.
[16] Dit valt reeds af te leiden uit de beperkte registratie van onderzoeken met persoonsgegevens in het register.
[17] Zogenaamde sets aan maatregelen worden momenteel beschreven en ontwikkeld bij RDO en worden "Building blocks" genoemd. Deze zijn voor de onderzoeker echter nog maar beperkt beschikbaar.

5. Doelbinding en intern toezicht

In het kader van de nieuwe, maar ook onder de voorgaande privacywetgeving, is verwerking van persoonsgegevens enkel toegestaan wanneer men een doel en grondslag heeft voor de verwerking. Het doel dient welomschreven en precies te zijn. Het hanteren van vage of hele brede doelen zijn in beginsel niet toegestaan.[18] Ook het (her)formuleren van een doel gedurende de verwerking is niet toegestaan, dit wordt ook wel doelbinding genoemd.

In de Algemene privacyverklaring Rijksuniversiteit Groningen ("privacyverklaring") zijn globaal de doelen van de verwerkingen bij de RUG vastgelegd. In het privacybeleid is het toezicht op het rechtmatig verwerken van persoonsgegevens neergelegd bij de faculteitsbesturen en directies. Het algemene interne toezicht is ingevuld middels de aanstelling van de FG.

Het volwassenheidsniveau op dit onderdeel binnen de RUG:

Algemene risico's

Het ontbreken van een grondslag of een welomschreven en precies doel bij de verwerking van persoonsgegevens leidt tot ongeoorloofd en onrechtmatig handelen. Onrechtmatige en ongeoorloofde verwerkingen kunnen ernstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene, maar ook consequenties[19] hebben voor de organisatie zelf.

Doelbinding

De RUG telt duizenden verwerkingen. Bij de RUG ontbreekt er op dit moment een eenduidige controle op de rechtmatigheid en doelen van alle bestaande en nieuwe verwerkingen.

Ook de FG heeft tot nu toe geen rol bij een structurele controle op de rechtmatigheid van de beschreven verwerkingen.

Een effectieve controle op de doelen van die verwerkingen kan enkel worden bereikt door:

1) op centraal niveau doelen en grondslagen van verwerkingen vast te stellen. Indien de RUG de doelen en grondslagen centraal vastlegt, kan intern toezicht worden gehouden op de rechtmatigheid ervan;

[18] Uitzonderingen kunnen onder strikte voorwaarden worden gemaakt bij onder meer onderzoek.
[19] Hierbij moet gedacht worden aan bestuurlijke boetes, imagoschade of verlies van vertrouwen door stakeholders.

2) de instellingsbrede doelen te koppelen aan gestandaardiseerde processen binnen de RUG. Het standaardiseren van processen zal tevens onderdeel uitmaken van het traject om te komen tot een functioneel register.

Faculteiten en diensten volgen in beginsel de standaardprocessen of dienen te verklaren waarom daarvan wordt afgeweken.[20] Controle ziet in dat geval met name op de naleving van de standaardprocessen.

Bij het formuleren van de doelen en grondslagen is het advies aan het CvB om zoveel mogelijk te leren van de sector en in sectorverband de grondslagen en doelen in te vullen. Hierin is een (grote) rol weggelegd voor de VSNU.

Dataminimalisatie gekoppeld aan doelbinding

In het verlengde van de doelen en grondslagen zal de RUG ook de toepassing van dataminimalisatie moeten bewaken. Dataminimalisatie is onlosmakelijk verbonden met de doelbinding; de RUG zou niet meer persoonsgegevens mogen verwerken dan strikt noodzakelijk is voor het doel van die verwerking.

Controle op dataminimalisatie wordt pas mogelijk indien de voornoemde standaardprocessen ook de te verwerken categorieën persoonsgegevens bevatten. Zo ontstaat het benodigde inzicht en overzicht.

Intern toezicht

Het interne toezicht is primair bij de FG belegd. De FG werkt veelal samen met de privacysectie van de afdeling Algemeen Bestuurlijke en Juridische Zaken (“ABJZ”) en de privacy- en securitycoördinatoren binnen de RUG.

In 2018 waren veel van de taken van de FG uitvoerend van aard en was toezichthouden beperkt mogelijk. Dit is voor een korte periode onoverkomelijk gezien het volwassenheidsniveau waarop de RUG acteerde[21]; toezichthouden op een afwezige privacymanagementorganisatie heeft geen toegevoegde waarde voor de bescherming van de betrokkenen en het vrije verkeer van gegevens.

Eind 2018, begin 2019 kreeg de FG met de verdere uitrol van de verantwoordelijkheden bij de faculteiten en diensten meer ruimte beschikbaar om als toezichthouder op te treden. Ook de (tijdelijke) personele uitbreiding bij ABJZ heeft hieraan bijgedragen.

[20] Meer over de gestandaardiseerde processen in Hoofdstuk 6.
[21] Het gemiddelde van de volwassenheidsniveaus bij de RUG bevond zich tussen de 0.0 en 1.0.

Desondanks is het nog onmogelijk gebleken om alle wettelijke taken binnen de RUG uit te voeren. Zo is gebleken dat de FG niet toekomt aan de beoordeling van alle DPIA's die worden uitgevoerd. Het beroep dat de organisatie op de FG doet als adviseur op het gebied van gegevensbescherming is van dusdanige omvang dat niet alle (wettelijke) taken voldoende aandacht kunnen krijgen.

Op het moment dat privacy- en securitycoördinatoren de benodigde kennis over de privacybeginselen hebben opgedaan en deze in de praktijk kunnen toepassen, zal het beroep van de organisatie op de FG (en de privacysectie bij ABJZ) vermoedelijk kleiner worden.

Verder is het noodzakelijk om de tijdelijke ondersteuning van de FG en de privacysectie van ABJZ structureel te maken. Intern toezichthouden is niet mogelijk wanneer de FG het werk van privacyjuristen uitvoert. Op hun beurt kunnen de privacyjuristen hun taak niet goed uitvoeren wanneer zij geconfronteerd worden met de afhandeling van vele administratieve werkzaamheden.

6. Register

Een van de nieuwe verplichtingen die de AVG brengt, betreft het register (art. 30 AVG). Het register dient een overzicht te geven van de verwerkingen die de RUG als verantwoordelijke uitvoert. Op verzoek van de Autoriteit Persoonsgegevens ("AP") dient de RUG dit overzicht van verwerkingen te kunnen overdragen.

De RUG heeft een uitgebreid register opgezet waarbij alle faculteiten en diensten input hebben geleverd. Het register wordt momenteel beheerd in de zogenaamde Research Data Management Plan-tool ("RDMP-tool"). De RDMP-tool bevat nu circa 2.000 verwerkingen.

Ook zal de RUG de registertool *Privacy Perfect* verder implementeren. Privacy Perfect moet hét centrale systeem zijn dat de verwerkingen binnen de domeinen Onderwijs en Bedrijfsvoering in kaart moet hebben. De RDMP-tool blijft bestaan voor de verwerkingen binnen onderzoek. Beide systemen gezamenlijk geven de RUG in principe een overzicht van alle verwerkingen van persoonsgegevens.

Richtlijnen voor de invulling en beheer van het register zijn in ontwikkeling, maar nog niet formeel op centraal niveau vastgesteld. Het ontbreken van vastgestelde richtlijnen heeft tot gevolg dat de RUG lastig aan haar informatieplicht kan voldoen (zie hoofdstuk 10) en het kwaliteitsmanagement niet optimaal kan plaatsvinden (zie hoofdstuk 7).

Het volwassenheidsniveau op dit onderdeel binnen de RUG:

Algemene risico's

Het ontbreken van een volledig en actueel register van verwerkingen leidt tot een incompleet overzicht van categorieën van betrokkenen en type persoonsgegevens, maar ook tot het ontbreken van een volledig overzicht van de toegepaste technische en organisatorische maatregelen voor essentiële en gevoelige verwerkingen. Op verzoek van de Autoriteit Persoonsgegevens kan vanzelfsprekend ook geen volledig en actueel overzicht worden overgedragen.[22]

Technische en organisatorische invulling van het register

Met het gebruik van de RDMP-tool wordt tegemoetgekomen aan de onderzoekers die de RDMP-tool al moeten gebruiken voor hun datamanagementplan en de daarbij behorende

[22] Een verplichting daartoe is te vinden in art. 30 lid 4 AVG.

ethische vragen die zij beantwoorden. De administratieve last voor de onderzoeker wordt met het aanhouden van dit systeem dus beperkt.

Met de opzet van het register in de RDMP-tool zet de RUG een eerste stap richting compliance voor wat betreft deze eis uit de AVG. Het register voldoet echter nog niet aan alle vereisten.

Het register bevat nog niet voor alle beschreven verwerkingen de bewaartermijnen en omschrijving van de technische en organisatorische beveiligingsmaatregelen. Hier zal de RUG in 2019 op centraal niveau een eenduidige werkwijze voor moeten opstellen.

Het advies is om op centraal niveau gestandaardiseerde processen[23] vast te stellen die in beginsel moeten worden gevolgd binnen de RUG. Bij de vormgeving van deze processen wordt een minimum aan beveiligingsmaatregelen en de maximale bewaartermijnen omschreven.

Beveiligingsmaatregelen en bewaartermijnen

Binnen het Research Data Office (“RDO”) en ABJZ wordt gewerkt aan voorgedefinieerde sets aan beveiligingsmaatregelen, “Building Blocks”. Hiermee kan op basis van het risicoprofiel van een verwerking gekozen worden voor een specifieke set aan Building Blocks.

Wat betreft de bewaartermijnen zal er in 2019 aansluiting gezocht moeten worden bij de sectorale Selectielijst voor universiteiten. Deze wordt in het voorjaar van 2019 verwacht. Tot die tijd geeft de Selectielijst voor de hogescholen een goed kader voor de invulling van bewaar-/verwijdertermijnen.

Onderzoeken zijn niet geregistreerd en inzichtelijk

Een risico voor het komen tot compliance op dit punt vormen de wetenschappelijke onderzoeken binnen de RUG.

Faculteiten hebben niet in kaart welke onderzoeken (met persoonsgegevens) worden uitgevoerd. Een onderzoek dat niet bekend is bij de interne organisatie, is tevens niet te ondersteunen voor wat betreft beveiligingsmaatregelen, bewaartermijnen en het contracteren van derde partijen.

De RUG heeft op centraal, maar tevens op decentraal niveau nog geen concreet plan om tot een volledig overzicht van de verwerkingen binnen onderzoek te komen.[24]

De faculteiten zijn verantwoordelijk voor onderzoek en de inventarisatie van onderzoeken. Zij dienen in samenspraak met RDO een plan op te stellen om te komen tot een volledig overzicht van verwerkingen in onderzoek.

[23] De gestandaardiseerde processen worden gebaseerd op de thans geregistreerde verwerkingen.
[24] Zie hiervoor ook de opmerkingen in hoofdstuk 4 onder “Onderzoek(ers)”.

Gezamenlijk register RUG-UMCG

De RUG en het UMCG zijn met betrekking tot onderzoek en onderwijs sterk verweven. In het kader van die samenwerking is een Raamovereenkomst gesloten waarin is afgesproken om te komen tot een gezamenlijk register.

Om tot een legale en effectieve symbiose te komen, zullen er nog enkele zaken ten aanzien van de verwerking van persoonsgegevens moeten worden geconcretiseerd. In 2016 hebben de RUG en het UMCG een samenwerkingsovereenkomst gesloten ten aanzien van de verwerking van persoonsgegevens.[25]

Daarbij zou een gezamenlijk register worden opgezet. Dit laatste is echter nog niet gerealiseerd en onduidelijk is wie hier verantwoordelijk voor is.

Zolang afspraken niet uitgewerkt worden en onduidelijkheid bestaat over welke partij wat verwerkt en met welk doel, bestaat de kans op onrechtmatige verwerking en verlies van persoonsgegevens.

Momenteel zijn er overleggen gaande tussen de RUG en het UMCG om verdere invulling te geven aan de Raamovereenkomst.[26] Een concrete invulling dient in 2019 vorm te krijgen, wil de Raamovereenkomst gevolgd worden.

Los van de bestaande overleggen dient de RUG één of meerdere verantwoordelijken aan te wijzen die bewaken dat de doelen uit de Raamovereenkomst worden nageleefd.

[25] De RUG en het UMCG staan op het punt om een nieuwe versie van de samenwerkingsovereenkomst te tekenen.
[26] Bij de gesprekken zijn de FG's (UMCG & RUG), security manager (RUG) en IT-jurist (RUG) betrokken.

7. Kwaliteitsmanagement

Bij kwaliteitsmanagement gaat het om processen die enerzijds de juistheid en nauwkeurigheid van persoonsgegevens bewaken. Anderzijds gaat kwaliteitsmanagement over het rectificeren, vervolledigen, verwijderen en beperken van de verwerking van persoonsgegevens wanneer persoonsgegevens niet juist of onnauwkeurig zijn.

Het niveau van kwaliteitsmanagement binnen de RUG is sterk afhankelijk van de categorie betrokkene en de plaats binnen de organisatie. De drie belangrijkste categorieën zijn studenten, medewerkers en deelnemers bij onderzoek ("onderzoekssubjecten"). Per categorie betrokkene zal de invulling van het kwaliteitsmanagement beschreven worden.

Dit hoofdstuk zal met name aandacht besteden aan de juistheid en nauwkeurigheid van persoonsgegevens en de mogelijkheid om deze te rectificeren. Verzoeken om verwijdering van persoonsgegevens zijn bij de RUG minder relevant en worden daarom niet beschreven.[27]

Het volwassenheidsniveau op dit onderdeel binnen de RUG:

Algemene risico's

In het geval incorrecte persoonsgegevens worden verwerkt, kan dit leiden tot verkeerde conclusies over de betrokkene met negatieve gevolgen van dien. Denk hierbij aan een verkeerd afgegeven BSA of verzending van HR-documenten naar het oude en daarmee verkeerde adres.

Persoonsgegevens van studenten

Voor wat betreft studenten ontvangt de RUG continu updates vanuit het systeem Studielink met de laatste stand van zaken omtrent hun persoonsgegevens. De studentgegevens komen bij de RUG binnen in Progress.NET. Studielink synchroniseert op haar beurt weer met de Basisregistratie Personen, DUO en IND.

Hiermee wordt gewaarborgd dat de RUG de gegevens die zij verwerkt van haar studenten te allen tijde actueel zijn. Vanuit Progress.NET worden de persoonsgegevens binnen de RUG doorgezet en gesynchroniseerd met andere systemen. Voor dit gedeelte van de keten borgt de RUG de juistheid en nauwkeurigheid effectief.

[27] Het recht op verwijdering kent enkele uitzonderingen, zo ook verwerkingen die plaatsvinden in het kader van een taak van algemeen belang. De RUG verwerkt de meeste studentgegevens op basis van die grondslag.

Verder in de keten worden de hierboven genoemde systemen gebruikt om persoonsgegevens te exporteren naar onder meer Excel-bestanden.[28] Dit is binnen de RUG eerder norm dan uitzondering. Het is vanzelfsprekend dat het gemiddelde Excel-bestand géén dagelijkse synchronisatie kent met één van de systemen. Per definitie werkt de RUG dus in dat gedeelte van de keten met persoonsgegevens die niet actueel en in sommige gevallen incorrect zijn.

Het advies is om het gebruik buiten de gebaande paden (lees: de bedrijfssystemen) eerst in kaart te brengen en te onderzoeken in welke behoefte deze alternatieve systemen voorzien, alvorens deze eventueel te vervangen met functionaliteit in de gecertificeerde bedrijfssystemen.

Correctie persoonsgegevens studenten

Een student kan de meest basale persoonsgegevens laten wijzigen in de Basisregistratie Personen ("BRP") van de overheid en in het systeem Studielink. Studenten die zijn ingeschreven in de BRP, kunnen voor authenticatie in Studielink hun DigID gebruiken. Op die manier wordt met grote zekerheid de identiteit van de student vastgesteld.

Studenten zonder inschrijving in de BRP dienen zich na wijziging van persoonsgegevens in Studielink te identificeren bij de balie van de Centrale Studenten Administratie, voordat wijzigingen vanuit Studielink worden overgenomen in Progress.NET.

De controle op de identiteit van deze studenten wordt gedaan middels de (buitenlandse) paspoorten en ID-kaarten. Dit is momenteel een handmatig proces en is derhalve onderhevig aan een (menselijke) foutmarge.

Om buitenlandse paspoorten met grotere zekerheid te kunnen verifiëren op echtheid, wordt er momenteel een project gestart binnen Studenten Informatie en Administratie ("SIA") om middels intelligente scanners de echtheid van identiteitsbewijzen met 99,99% zekerheid te verifiëren. Een dergelijke handelswijze zou 1) een accuratere controle opleveren en 2) veel uren besparen van medewerkers.

Persoonsgegevens van medewerkers

Voorafgaand aan de aanstelling leveren medewerkers hun gegevens aan. Na de aanstelling hebben medewerkers de mogelijkheid om hun persoonsgegevens deels aan te passen middels het gebruik van de portal Do It Yourself en/of middels (telefonisch) contact met HR-Services. De volledigheid en actualiteit van deze gegevens wordt hiermee geborgd.

[28] Een dergelijk beeld wordt geschetst door eigenaren en beheerders van de systemen, maar ook bevestigd door de decentrale studentenadministraties.

De basisset aan persoonsgegevens van medewerkers wordt beheerd in Peoplesoft. Vanuit Peoplesoft worden andere (HR-)systemen gevoed en wordt ook teruggekoppeld.

Voor persoonsgegevens van medewerkers zal het project BP 2020 uitkomst kunnen bieden. BP 2020 heeft geleid tot de aanschaf van het softwarepakket AFAS. AFAS ziet op het beheer en de optimalisatie van administratieve processen. AFAS biedt onder meer workflows om de kwaliteit van gegevens te bewaken en te borgen. Het systeem bevat ook gestandaardiseerde en op-maat gemaakte waarschuwingen om foutmarges in processen te verkleinen.

Het mag duidelijk zijn dat voorafgaand aan de implementatie van AFAS, de (nieuwe) protocollen/werkwijzen rondom de verwerking van persoonsgegevens moeten zijn vastgesteld. De uiteindelijke bewaking en borging van de kwaliteit van persoonsgegevens valt of staat met het aanwezige beleid en de naleving daarvan.

Een structurele aanpak van processen zoals in BP 2020 is gebeurd, is op het gebied van onderwijs ook vereist om de ongewenste verwerkingen in Excel-documenten tegen te gaan.

Persoonsgegevens van onderzoekssubjecten

Het beheer van data in onderzoek wordt bij de RUG beschreven in datamanagementplannen. Deze plannen zien niet specifiek op de bescherming van persoonsgegevens, maar zien op belangrijke uitgangspunten als transparantie en verifieerbaarheid van onderzoek en hergebruik van onderzoeksgegevens.[29] Veelal komt de bescherming van persoonsgegevens pas aan bod bij de fase “toegang verschaffen tot data”.[30]

De RUG heeft geen specifieke richtlijnen ten behoeve van de kwaliteitsmanagement van persoonsgegevens in onderzoek.[31] De Gedragscode WI en de Gedragscode voor gebruik persoonsgegevens in wetenschappelijk onderzoek[32] (“Gedragscode persoonsgegevens onderzoek”) behandelen dit aspect wel.

De Gedragscode persoonsgegevens onderzoek is voor wat betreft het aspect kwaliteitsmanagement nog geen integraal onderdeel van de onderzoeksmethodiek bij de RUG. Omgang met verzoeken tot rectificatie of verwijdering van persoonsgegevens is niet (de)centraal vastgesteld.

Binnen HSR is de handleiding “Starting with a DPIA methodology for human subject research” opgesteld voor het uitvoeren van een DPIA in onderzoek. In de handleiding wordt het aspect datakwaliteit behandeld en toegelicht voor de onderzoeker.
Het advies is derhalve om de handleiding, dan wel aspecten hiervan, onderdeel te maken van het curriculum en de voorbereiding van onderzoek met persoonsgegevens.

[29] M. van Berchum, & M.J. Grootveld, ‘Het beheren van onderzoeksdata’, *Handboek Informatiewetenschap*, IV B 475, Vakmedianet, 2016, p. 2-3.
[30] M. van Berchum, & M.J. Grootveld, ‘Het beheren van onderzoeksdata’, *Handboek Informatiewetenschap*, IV B 475, Vakmedianet, 2016, p. 16-17.
[31] Uitzondering hierop is het WMO-plichtig onderzoek dat gezamenlijk met het UMCG wordt uitgevoerd.
[32] De gedragscode stamt uit 2005 en is verouderd. Er wordt vanuit de VSNU gewerkt aan een nieuwe gedragscode.

8. Bewaren van persoonsgegevens

Op grond van de AVG is de RUG verplicht om persoonsgegevens niet langer te bewaren dan strikt noodzakelijk is voor het doel van de verwerking. Dat betekent dat na het bereiken van een specifieke bewaartermijn persoonsgegevens moeten worden verwijderd of geanonimiseerd. Na het anonimiseren van gegevens wordt er niet meer gesproken van persoonsgegevens en is de AVG dus niet langer van toepassing.

Binnen de drie grote categorieën van betrokkenen (studenten, medewerkers en onderzoekssubjecten) is de omgang met bewaartermijnen verschillend ingericht bij de RUG.

Het volwassenheidsniveau op dit onderdeel binnen de RUG:

Algemene risico's

Het risico van het langer bewaren van persoonsgegevens dan strikt noodzakelijk is dat persoonsgegevens kunnen worden verwerkt voor andere doelen dan de oorspronkelijke doelen. Hiermee zou er in strijd met de doelbinding worden gehandeld en kan er sprake zijn van onrechtmatig handelen.

Persoonsgegevens studenten

Binnen de RUG zijn de bewaartermijnen voor documenten die studentgegevens bevatten bekend. Middels het Project Digitaal Student Dossier ("Project DSD") wordt geprobeerd om de bewaartermijnen op een uniforme organisatiebrede wijze vast te stellen en toe te passen.

Project DSD vormt een goede stap richting een beargumenteerde en geïmplementeerd beheer van bewaartermijnen. Het verhogen van het volwassenheidsniveau valt of staat met het al dan niet implementeren van Project DSD binnen de gehele RUG.

Risico's voor de RUG op dit onderdeel liggen op het niet-volgen van de gestandaardiseerde vastgestelde processen. Bij afwijking van deze processen worden applicaties als Excel of Outlook gehanteerd, welke het beheer en naleving van bewaartermijnen praktisch onmogelijk maken.[33]

[33] Meer over de gestandaardiseerde processen in Hoofdstuk 5 Doelbinding en intern toezicht.

Persoonsgegevens medewerkers

Voor het overgrote gedeelte van de persoonsgegevens van het personeel zijn bewaartermijnen bekend. De bewaartermijnen worden tot dusver niet of beperkt nageleefd; de relevante systemen zijn daar niet voor ingericht.[34]

De komst van BP 2020 maakt het mogelijk om persoonsgegevens van personeel te verwijderen bij het bereiken van het einde van een bewaartermijn.

Gezien het vele maatwerk in de dienstverbanden bij de RUG, is het (geheel) geautomatiseerd verwijderen van persoonsgegevens vooralsnog geen veilige optie. Zonder handmatige controle bestaat de kans op het per ongeluk verwijderen van persoonsgegevens. Indien deze nog op een gerechtvaardigde wijze werden verwerkt, kan dat een datalek opleveren.

Het technisch inregelen van bewaar- en verwijdertermijnen zal initieel een grote opdracht zijn, maar daar ligt niet het grootste risico. Het organisatorisch inregelen van het tijdig verwijderen van persoonsgegevens is hetgeen waar de RUG zich op moet focussen.

Het opstellen van de zogenaamde ‘best practices’ en het duidelijk formuleren van verantwoordelijkheden is daarbij essentieel wil de RUG de bewaartermijnen goed naleven.

Persoonsgegevens onderzoekssubjecten

Voor persoonsgegevens in onderzoek gelden afwijkende regels ten opzichte van de hierboven benoemde verwerkingen. Zo maakt de AVG het mogelijk om in het geval van wetenschappelijk onderzoek af te zien van het verbod op het eeuwigdurend bewaren van persoonsgegevens. Voorwaarde is wel dat de verantwoordelijke passende maatregelen neemt om de gegevens te beschermen. Het pseudonimiseren van persoonsgegevens is een voorbeeld van een dergelijke maatregel.

Binnen de RUG is geen sectorspecifiek of instellingsbreed beleid omtrent de bewaartermijnen van persoonsgegevens in onderzoek. Onderzoekers zijn op dit moment aangewezen op de eigen interpretatie van de gedragscodes[35] en de privacywetgeving.

Belangrijk is om per sector/onderzoeksgebied te kijken naar de redenen (lees: doelen) om persoonsgegevens lang(er) te bewaren. De meest voor de hand liggende zijn: 1) voor de toepassing in nieuw onderzoek en; 2) voor replicatie en verificatie van het initiële onderzoek.

Het advies is om op centraal niveau kaders te schetsen die per faculteit (of onderzoeksgebied) ingevuld dienen te worden. Op die wijze kunnen sectorspecifieke richtlijnen vorm krijgen. Bij het opstellen is de inbreng van onderzoekers cruciaal.

[34] ImageNow en DIS bevatten veel oude personeelsdossiers. Met ImageNow zou het in technische zin mogelijk zijn om bewaartermijnen na te leven; met BP 2020 op komst lijkt dat echter overbodig.
[35] Bewaartermijnen zijn uit de Gedragscode WI gehaald. In de voorganger, de Nederlandse Gedragscode Wetenschapsbeoefening, stond wel een minimale bewaartermijn van tien jaar voor ruwe onderzoeksgegevens.

9. Beveiligen van persoonsgegevens

De AVG vraagt van de verantwoordelijke om ten behoeve van de verwerking van persoonsgegevens passende technische en organisatorische maatregelen te treffen.[36] Die beveiligingsmaatregelen zijn preventief, repressief en correctief van aard. Ook procedures en processen die gevolgen van beveiligingsincidenten kunnen beperken of voorkomen vallen hieronder. Met de term "passend" doelt de AVG op maatregelen die rekening houden met de stand van de techniek, uitvoeringskosten, maar ook de aard, omvang en context van de verwerkingen en hun doelen.

De RUG heeft tot op het heden de beveiligingsrisico's niet structureel in beeld gebracht. De risico's en mitigerende maatregelen worden enkel op informeel niveau en naar keuze van de interne verantwoordelijke vastgesteld.

Het volwassenheidsniveau op dit onderdeel binnen de RUG:

Algemene risico's

Bij de afwezigheid van (passende) beveiligingsmaatregelen zijn persoonsgegevens te manipuleren of te misbruiken. Ook kan het zijn dat persoonsgegevens niet langer beschikbaar zijn of per abuis publiekelijk bekend worden. Verder dient bij een gebrek in de beveiliging de betrokkenen eerder te worden geïnformeerd in het geval van datalekken.

De RUG beschikt over een Information security baseline ("Baseline") waarin het minimale niveau van beveiligingsmaatregelen is beschreven. De naleving van de Baseline wordt echter nog niet meegenomen in de RUG-brede PDCA-cyclus.

In 2019 dient de RUG bij de (interne) werkplannen voor privacymanagement ook de beveiliging op te nemen. Door beveiliging onderdeel te maken van de bestuurlijke cyclus wordt de Baseline ontheven van haar status als "papieren tijger".

Naast de meer algemene lijn van beveiligingsmanagement, kent de RUG een aantal relevante onderwerpen die variëren van intern gebruik van persoonsgegevens tot gebrekkige beveiliging bij verwerkers. De meeste relevant en urgente onderwerpen worden hieronder beschreven.

[36] De eis van passende technische en organisatorische maatregelen wordt gevonden in artikel 32 AVG.

Verwerking persoonsgegevens op de werkvloer

Verreweg de meeste “winst” op het gebied van beveiliging is te behalen op de werkvloer en niet per se binnen één van de grote administratieve systemen. Hieronder worden enkele risico’s benoemd en oplossingen voorgesteld.

Onbeveiligde verwerking van (bijzondere) persoonsgegevens

De communicatie tussen faculteiten en overige diensten binnen de RUG verdient enige aandacht. Er worden momenteel documenten met grote aantallen (bijzondere) persoonsgegevens intern onbeveiligd verzonden. Een voorbeeld hiervan is de onbeveiligde verzending van identiteitsbewijzen aan de afdeling SIA.

Een relatief eenvoudige oplossing voor het onbeveiligd verzenden van dergelijke documenten, kan liggen in het gebruik van encryptie en/of het delen van bestanden via een gedeelde beveiligde schijf. De digitale mogelijkheden voor veilige verzending zijn aanwezig, maar het ontbreekt de RUG aan richtlijnen.

Het vaststellen van richtlijnen rondom de veilige verzending van (bijzondere) persoonsgegevens en het helder communiceren van deze richtlijnen naar de medewerkers moet leiden tot een algehele groei in de beveiliging van persoonsgegevens. Bewustwording bij de medewerker is onmisbaar voor die groei.

Met voornoemde oplossing wordt tevens een deel van de problematiek rondom de reguliere e-mail opgelost. E-mail is in het algemeen een risico voor de bescherming van persoonsgegevens. De naleving van bewaartermijnen, grondslagen en doelen zijn binnen de e-mailbox van medewerkers niet te controleren.

BYOD

Het gebruik van eigen apparaten (Bring your own device) werd binnen de RUG gestimuleerd, o.a. door de zogenaamde Tabletregeling. Medewerkers maken massaal gebruik van hun eigen telefoon, tablet of laptop om werkzaamheden voor de RUG te verrichten. Hieronder valt vanzelfsprekend de verwerking van (bijzondere) persoonsgegevens.

Het is onbekend of en op welke wijze deze BYOD zijn beveiligd. Het toezicht op de inrichting van de BYOD en de naleving van de Baseline met betrekking tot deze BYOD is bij de RUG zo goed als afwezig.

De gevolgen hiervan worden duidelijk wanneer dergelijke apparaten verloren of gestolen worden; datalekken met (bijzondere) persoonsgegevens dienen gemeld te worden bij de AP en meestal ook bij de betrokkenen.

Een eerste stap in het mitigeren van dit risico ligt in de informatieverstrekking rondom veilig gebruik van BYOD bij huidige en nieuwe medewerkers. Daarnaast is controle op de naleving van de Baseline met betrekking tot BYOD gewenst.

Registratie uitgegeven apparaten

Naast de meegebrachte apparatuur worden bij de RUG grote aantallen apparaten, zoals laptops, ter beschikking gesteld aan medewerkers. In overeenstemming met de Baseline zouden deze apparaten na het einde van het dienstverband van de medewerker –of- bij de buitengebruikstelling van het apparaat zelf, moeten worden geformatteerd en/of worden vernietigd.

Registratie van ter beschikking gestelde apparaten ligt momenteel bij het Facilitair Bedrijf. De registratie is echter niet volledig en wordt door de intern verantwoordelijken niet consequent bijgehouden. De RUG zou ter bescherming van persoonsgegevens in kaart moeten hebben waar de uitgegeven apparaten zich bevinden. Controle op deze apparaten dient derhalve onderdeel uit te maken van het exit-protocol bij de RUG.

Een gunstig neveneffect van een nauwkeurigere registratie van apparaten kan daarnaast liggen in het beperken van fraude en/of verduistering.

Versleuteling uitgegeven apparaten

Een eerste stap om de beveiliging van (uitgegeven) apparaten te verbeteren vormt het Project versleutelen gegevensdragers. Middels het project wordt de infrastructuur opgeleverd om universiteitsbreed desktop pc's en laptops te versleutelen. De verwachte oplevering van de infrastructuur: Q2 2019.

Binnen de scope van het Project vallen enkel de desktop pc's en laptops. Buiten de scope valt de bescherming, dan wel versleuteling, van tablets en andere mobiele apparatuur die persoonsgegevens verwerken. Gezien het feit dat de gemiddelde medewerker één of meerdere (persoonlijke) apparaten hanteert voor de werkzaamheden binnen de RUG, levert dit nog steeds een hoog risico op voor de bescherming van persoonsgegevens.

Het Project versleutelen gegevensdragers regelt enkel de technische implementatie van beveiligingsmaatregelen. Het project zal pas effectief zijn wanneer de RUG ook organisatorische maatregelen neemt en ervoor zorgt dat medewerkers met een (zakelijke) laptop worden aangespoord om deze te (laten) versleutelen. Het advies is derhalve om te kijken naar de organisatorische kant en HR hierbij te betrekken.

De-identificeren van persoonsgegevens bij onderzoek

Een beveiligingsmethodiek bij onderzoek is het pseudonimiseren of anonimiseren van persoonsgegevens. Met pseudonimiseren worden de risico's voor betrokkenen verminderd. De bruikbaarheid van de data blijft hoog, terwijl de risico's binnen de perken blijven.

Ook draagt pseudonimiseren bij aan het voldoen aan verplichtingen inzake de bescherming van persoonsgegevens, waaronder de passende beveiligingsmaatregelen.

Daarnaast hoeft de RUG bij sterke pseudonimisering niet langer te voldoen aan verzoeken van betrokkenen.[37]

Geanonimiseerde gegevens worden onder de AVG niet langer gezien als persoonsgegevens. De verwerking van anonieme gegevens valt derhalve niet langer onder de AVG.

Om onderzoek beter te beveiligen dient de RUG de onderzoeker technisch en organisatorisch te ondersteunen bij het pseudonimiseren en anonimiseren.

Beveiliging Progress.NET

Naast de risico's door het gebruik van apparatuur en bij onderzoek, kent de RUG een aantal grote en voor de bedrijfsvoering cruciale applicaties. Hieronder vallen onder meer PeopleSoft, INFOR en Progress.NET. Met de komst van BP 2020 worden de risicovolle processen in de eerste twee applicaties beperkt of weggenomen, daarom worden enkel de risico's in Progress.NET beschreven.

Progress.NET is het systeem dat binnen de RUG de meeste persoonsgegevens van studenten verwerkt. Naast naam, adres, tentamencijfers en judicia worden bijvoorbeeld ook notities van studieadviseurs en zelfs psychologen beheerd in Progress.NET.

Gezien de omvang en de mate van gevoeligheid van de gegevens heeft het passend beveiligen van de persoonsgegevens in dit systeem een hoge prioriteit. Op dit moment kent Progress.NET en het bedrijf achter de applicatie, UOCG Market BV, enige aandachtspunten op het vlak van het beveiligen van persoonsgegevens. De drie belangrijkste punten worden aangestipt.

Allereerst zijn rollen en rechten binnen het systeem nog niet op een verfijnde manier in te richten. Dit resulteert in toegang tot meer of minder persoonsgegevens dan strikt noodzakelijk is voor medewerkers.

Ten tweede is uit een recent overzicht gebleken dat meerdere (10+) ontwikkelaars toegang hebben tot zeer gevoelige en bijzondere persoonsgegevens van studenten.[38]

De RUG dient te beoordelen of toegang tot bijzondere persoonsgegevens door ontwikkelaars noodzakelijk is en dient te sturen op minder risicovolle wijzen van ontwikkeling.

[37] Een betrokkene is voor de RUG namelijk niet langer te koppelen aan de gegevens die zij verwerkt.
[38] Het overzicht is afkomstig uit de Faculteit Rechtsgeleerdheid en toont aan dat meer ontwikkelaars dan medewerkers toegang hebben tot psychologennotities van studenten bij de RUG.

Het derde punt ziet op de wijze van testen. Alle versies van Progress.NET worden tot op heden bij de ontwikkelaar getest met de daadwerkelijke data van onze studenten (“live data”). Testen met live data is enkel in uitzonderlijke gevallen toegestaan.[39]

Er zijn alternatieven voor het testen met live data waar een gelijkwaardig resultaat mee kan worden bereikt. Hierover dient de RUG afspraken te maken met UOCG Market BV.

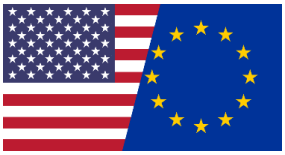
De CLOUD Act

Naast externe risico’s in de vorm van verwerkers, kent 2018 ook een belangrijke wijziging in de buitenlandse wetgeving. In 2018 is namelijk de Amerikaanse CLOUD Act aangenomen.

Bij de beveiliging van gegevens dient de RUG rekening te gaan houden met die CLOUD Act. Deze Act verplicht Amerikaanse bedrijven om op verzoek van de Amerikaanse autoriteiten data die buiten de VS op servers zijn geplaatst aan te leveren.[40] Partijen als Microsoft en Google vallen onder de CLOUD ACT. In veel gevallen worden de desbetreffende bedrijven verplicht tot geheimhouding van die vordering tot het overdragen van data.

Een vordering tot het overdragen van persoonsgegevens conflicteert in beginsel met de Europese privacyverordening.[41] De CLOUD Act maakt het wel mogelijk om als land een verdrag te sluiten met de VS om afspraken te maken over de invulling van de CLOUD Act. Een verdrag met Nederland is er tot dusver niet.

De Nederlandse overheid wijst naar de EU om een verdrag te sluiten. Zolang een dergelijk verdrag niet gesloten is, dient de RUG bij het inzetten van Amerikaanse verwerkers rekening te houden met de risico’s van de CLOUD Act voor de bescherming van persoonsgegevens.



[39] Testen met live data is enkel in die gevallen toegestaan waarin geen aantoonbaar alternatief aanwezig is.
[40] Hierover schrijft minister Ferd Grapperhaus op 5 oktober 2018 in een kamerbrief: “[..] Dit betreft in het bijzonder inhoudsgegevens zoals inhoud van e-mails, documenten, foto’s en video’s, etc. [..]”
[41] De verstrekking van persoonsgegevens aan een overheidsinstantie buiten de EU, zonder een internationale overeenkomst als grondslag, is verboden op grond van art. 48 AVG.

10. Informatieverstrekking en rechten betrokkenen

Organisaties die persoonsgegevens verwerken, zijn verplicht om de personen waarop de persoonsgegevens betrekking hebben ("de betrokkenen") daarover te informeren. Dit geldt ook in het geval de persoonsgegevens van derden zijn ontvangen. De betrokkenen hebben op hun beurt een aantal rechten om (beperkte) controle te kunnen uitoefenen op die persoonsgegevens. Hieronder vallen onder meer het recht op inzage, rectificatie, vergetelheid en bezwaar.[42]

De RUG heeft een algemene privacyverklaring. Deze omschrijft de verwerkingen van persoonsgegevens binnen de RUG op een hoog abstractieniveau.

Op een lager abstractieniveau zijn veel verwerkingen niet voldoende transparant gemaakt voor de betrokkenen. Betrokkenen zijn niet of beperkt bekend met de doelen, bewaartermijnen en beschermingsmaatregelen van die specifieke verwerkingen.
Ook worden privacyverklaringen van derden aan betrokkenen aangeboden terwijl niet die derden, maar de RUG de verantwoordelijke is.[43]

De RUG dient bij alle verwerkingen transparant te zijn richting de betrokkenen.

Het advies is om te starten met de meest omvangrijke en risicovolle verwerkingen en deze inzichtelijk te maken middels een privacyverklaring of andersoortige toelichting. Daarbij is communicatie op een beknopte, toegankelijk en begrijpelijk wijze van belang.

Het volwassenheidsniveau op dit onderdeel binnen de RUG:

Algemene risico's

Zonder transparantie kan een organisatie niet aantonen dat het voldoet aan alle privacybeginselen. Het niet-aantoonbaar voldoen aan die beginselen kan boetes of een last onder dwangsom opleveren. Daarnaast kan een gebrek aan transparantie afbreuk doen aan het vertrouwen in en reputatie van een organisatie.

[42] De belangrijkste rechten zijn opgenomen in artt. 15 – 22 AVG.
[43] Een voorbeeld hiervan is Blackboard; studenten zijn verplicht akkoord te gaan met de privacyverklaring en -voorwaarden van Blackboard alvorens toegang te krijgen tot de leeromgeving van de RUG.

Centraal Loket Privacy

Voor wat betreft het faciliteren in de rechten van de betrokkenen heeft de RUG het Centraal Loket Privacy ("Loket") ingericht. Betrokkenen kunnen daar een inzageverzoek of wijzigingsverzoek doen. In samenwerking met de privacy- en securitycoördinatoren wordt vanuit het Loket een antwoord geformuleerd en/of acties uitgezet.

Gezien de ondoorzichtigheid[44] van alle verwerkingen binnen de RUG is de bovenstaande exercitie zeer arbeidsintensief en is het tijdig[45] beantwoorden moeilijk.

Het Loket vervult een cruciale rol in de beantwoording van de vragen van betrokkenen. Belangrijk is daarom dat het Loket en de privacyverklaring van de RUG toegankelijk zijn en niet verborgen zijn voor de doelgroep.[46]

Aantallen inzageverzoeken en overige verzoeken

In 2018 heeft de RUG de volgende verzoeken op grond van de AVG ontvangen:

Recht op inzage:	**14**
Recht op verwijdering[47]:	**31**
Recht op dataportabiliteit:	**1**

Van deze verzoeken heeft de RUG **13** inzageverzoeken, **1** verzoek tot verwijdering en **1** verzoek tot dataportabiliteit in behandeling genomen nadat de desbetreffende betrokkene zich had geïdentificeerd. In de overige gevallen heeft de betrokkene zich niet geïdentificeerd en gaat de RUG derhalve niet over tot verstrekking of verwijdering van persoonsgegevens.

Persoonsgegevens betrokkenen in onderzoek

In het geval van verwerking van persoonsgegevens ten behoeve van onderzoek, kan er worden afgeweken van een aantal rechten van onderzoekssubjecten.[48] Zo kan de RUG besluiten om het onderzoekssubject geen inzage te geven in haar gegevens. Ook hoeft het recht op verwijdering niet te worden ingewilligd indien daardoor het onderzoek onmogelijk wordt of ernstig in gedrang dreigt te worden gebracht.[49]

[44] Dit volgt uit de niet-gestandaardiseerde invulling van het register (zie ook hoofdstuk 6).
[45] Conform art. 15 AVG heeft de RUG in principe één maand om te reageren op het verzoek van de betrokkenen. Bij een inzageverzoek betekent dat het overleggen van een compleet overzicht van alle verwerkte persoonsgegevens.
[46] De privacyverklaring en het Loket dienen toegankelijk te zijn vanaf de pagina http://rug.nl. Nu staan de relevante documenten en links in een lange opsomming dieper in de website onder "Rechten en plichten".
[47] In 30 van de 31 gevallen ging het om een geautomatiseerd verzoek tot verwijdering ("Data Removal Request").
[48] Het afwijken van enkele rechten van de betrokkenen wordt gevonden in art. 89 lid 2 AVG jo. art. 44 UAVG.
[49] Deze beperking van het recht op verwijdering wordt gevonden in art. 17 lid 3 sub d AVG.

De bovenstaande uitzonderingen en de handelwijze in het geval van (overige) verzoeken van onderzoekssubjecten is binnen de RUG niet beschreven voor onderzoek.

Indien onderzoekssubjecten verzoeken indienen bij de RUG, zal het verzoek wel worden behandeld door het Loket.

Doordat de registraties van onderzoek binnen de RUG (veelal) afwezig zijn, is het voldoen aan een verzoek van een onderzoekssubject een veeleisend proces of praktisch onmogelijk. Registratie van onderzoek, zoals vermeld in hoofdstuk 6, is daarom raadzaam.

Verder is onbekend of onderzoekers de onderzoekssubjecten wijzen op hun rechten en daarbij verwijzen naar het Loket. Handvatten voor privacyverklaringen en soortgelijke documenten zijn beperkt aanwezig in de faculteiten/graduate schools.

Bij de oplevering van diensten/producten uit HSR dient er aandacht geschonken te worden aan middelen voor onderzoekers om onderzoekssubjecten te informeren.

Verder valt op dat onderzoekers in sommige gevallen onterecht stellen dat de verwerkte gegevens anoniem zijn. Dit heeft grote gevolgen voor de bescherming van de persoonsgegevens; de AVG is namelijk niet van toepassing op anonieme gegevens.

Het (beter) informeren van onderzoekers over de definitie “persoonsgegevens” bij het registreren of opstellen van een datamanagementplan voorkomt dergelijke misverstanden.

11. Verwerkersovereenkomsten en doorgifte

Een verantwoordelijke die een derde partij inzet om in opdracht van haar persoonsgegevens te verwerken is verplicht een verwerkersovereenkomst met die partij af te sluiten. Hierin staan afspraken over de omgang met die persoonsgegevens. Naast deze overeenkomst is het een verantwoordelijke enkel toegestaan om persoonsgegevens buiten de EER te brengen indien de doorgifte met waarborgen is omkleed.

Bij de duizenden verwerkingen van de RUG worden veel derden ("verwerkers") ingezet om persoonsgegevens te verwerken. Voor deze verwerkers hanteert de RUG een standaard-verwerkersovereenkomst, gestoeld op het landelijke model van SURF.[50] Niet alle partijen waar de RUG persoonsgegevens mee uitwisselt, vallen onder de juridische verhouding verantwoordelijke-verwerker. Zo werkt de RUG veel samen met het UMCG waarbij er sprake is van een zogenaamde "gezamenlijke verantwoordelijkheid".[51]

Het volwassenheidsniveau op dit onderdeel binnen de RUG:

Algemene risico's

Indien een organisatie niet voldoet aan dit criterium is het niet duidelijk voor de eigen organisatie en/of de derde partij wat exact wordt verwacht bij de verwerking van persoonsgegevens. De kans bestaat dat persoonsgegevens onrechtmatig worden doorgegeven/verwerkt of onvoldoende worden beveiligd.

Ontbrekende verwerkersovereenkomsten

Met honderden verwerkers heeft de RUG (nog) geen verwerkersovereenkomsten gesloten. Er zijn derhalve géén afspraken over het melden van datalekken, de doelen van de verwerking(en), het inzetten van sub-verwerkers en de handelswijze bij contact met betrokkenen. Een dergelijke overeenkomst is op grond van de geldende wetgeving verplicht.[52]

De RUG dient zo spoedig mogelijk afspraken te maken met deze verwerkers, waarbij zij risicogebaseerd te werk moet gaan. Belangrijk is dat de RUG eerst in kaart brengt met welke verwerkers er nog (contractuele) afspraken moeten worden gemaakt. Het

[50] SURF is een coöperatie van universiteiten, hogescholen en mbo-instellingen die werken aan ICT-innovatie.
[51] Meer over de relatie met het UMCG in Hoofdstuk 6. Gezamenlijk register RUG-UMCG.
[52] De verplichting om een verwerkersovereenkomst te sluiten wordt gevonden in art. 28 lid 3 AVG.

gaat om minimaal honderden verwerkers, dus een planmatige aanpak om de afspraken te bewerkstelligen is noodzakelijk.

Beheer verwerkersovereenkomsten

Op verschillende plaatsen (centraal en decentraal) worden verwerkersovereenkomsten namens de RUG met verwerkers gesloten.[53] Een duidelijk overzicht én controle ontbreekt RUG-breed.

Het ontbreken van overzicht wordt veroorzaakt door een gebrek aan een vastgesteld en eenduidig beleid rondom contracteren. Ook zijn afspraken over het technisch inrichten van het beheer van contracten onduidelijk of simpelweg afwezig.

Op dit moment loopt er een project om de klassieke inkoopcontracten te inventariseren en te beheren. Het project wordt geleid door de PH-Middelen van de Faculteit Wijsbegeerte drs. M. Hids (en de werkgroep contractbeheer).

Eenzelfde aanpak is noodzakelijk voor de verwerkersovereenkomsten. In theorie zouden de scope en de middelen van het voornoemde project kunnen worden uitgebreid om ook andersoortige contracten, zoals verwerkersovereenkomsten, een beheerde en gestructureerde plek te geven.[54]

Naleving door verwerkers

In de standaard-verwerkersovereenkomst van de RUG wordt de verwerker gevraagd om specifieke beveiligingsmaatregelen te treffen. Als verantwoordelijke is de RUG verplicht om de naleving daarvan te (laten) controleren. Het advies is om de volgorde van deze controles te baseren op het risicoprofiel van de verwerker(s). Een dergelijke controle is tot dusver nog achterwege gebleven.[55]

Doorgifte buiten de EER

Naast de vele verwerkers, geeft de RUG ook veel persoonsgegevens door buiten de grenzen van de EER (de EU inclusief Noorwegen, Liechtenstein en IJsland). Dit gebeurt veel voor onderzoek, maar ook voor bedrijfsapplicaties waarvan de server bijvoorbeeld in de Verenigde Staten staat.

Het ontbreekt de RUG op dit moment aan richtlijnen die zien op de manier waarop omgegaan moet worden met de doorgifte van persoonsgegevens buiten de EER. De RUG dient derhalve te beginnen met het opstellen van richtlijnen voor doorgifte.
Deze richtlijnen of protocollen voorzien wat betreft de doorgifte van persoonsgegevens ook in alle mogelijke scenario's bij een (harde) Brexit.[56]

---

[53] Zelfs individuele medewerkers sluiten verwerkersovereenkomsten af waarbij de RUG in juridisch zin gebonden kan zijn.
[54] De scope dient vergroot te worden wat betreft het type overeenkomsten, maar ook protocollen/beleid dienen te worden geformuleerd omtrent omgang en beheer van overeenkomsten.
[55] ATP Business Travel B.V. schond de afspraken in de verwerkersovereenkomst en werd niet geaudit.
[56] De AVG geeft een limitatieve opsomming van toegestane scenario's bij de doorgifte van persoonsgegevens.

12. Datalekken

Met de komst van de Wet Meldplicht Datalekken in 2016 is een verplichting ontstaan om datalekken[57] bij de AP en betrokkenen te melden. De AVG laat deze verplichting ongewijzigd. Datalekken betreffen niet enkel de verloren USB-sticks met persoonsgegevens, maar betreffen vaker het (per ongeluk) delen van persoonsgegevens van studenten met andere studenten of medewerkers die deze persoonsgegevens niet mogen ontvangen.

Gemiddeld wordt er bij de RUG één (potentieel) datalek per twee weken gemeld. Dit duidt op enige bekendheid met het begrip en de noodzaak om te melden bij medewerkers en studenten. Het is belangrijk om daarbij te melden dat er een gradatie bestaat in de gevolgen die datalekken kunnen hebben. Naarmate de impact van het datalek groter wordt, wordt de noodzaak om te melden bij de AP en de betrokkenen groter.

Een vastgesteld datalekken-protocol is aanwezig en wordt nageleefd. Het protocol en het fenomeen “datalek” kennen echter nog niet genoeg bekendheid.[58] Meer bekendheid voor het protocol leidt naar verwachting tot de melding van meer datalekken.[59]

Medewerkers bekend maken met de procedure bij datalekken zal RUG-breed moeten worden opgepakt. Praktisch alle medewerkers komen namelijk in aanraking met persoonsgegevens. De procedure opnemen bij de introductie van nieuwe medewerkers zou een logische plek zijn, zoals vermeld in hoofdstuk 3 onder “Kennis personeel”.

Het volwassenheidsniveau op dit onderdeel binnen de RUG:

Algemene risico’s

Datalekken kunnen negatieve gevolgen hebben voor de levenssfeer van betrokkenen (medewerkers, studenten en onderzoekssubjecten). Dit uit zich bijvoorbeeld in de vorm van discriminatie, identiteitsfraude en uitsluiting. Daarnaast kan de publicatie van datalekken een negatief effect hebben op de reputatie van de RUG binnen het onderzoeksveld en onderwijs.

[57] De AVG kent de term “datalek” niet, maar spreekt van “inbreuk in verband met persoonsgegevens”. Ten behoeve van de leesbaarheid wordt echter de term “datalek” gehanteerd.
[58] Datalekken worden niet altijd gemeld en komt de FG op het spoor middels informeel contact met collega’s.
[59] Na de bijeenkomsten over de AVG wordt een piek in het aantal meldingen van datalekken geconstateerd.

Met de groei van het volwassenheidsniveau van de RUG, zal het aantal datalekken vrijwel zeker afnemen. Tot die tijd ontbreekt het bij de RUG aan richtlijnen om (veelvoorkomende) datalekken te voorkomen. Er wordt vooralsnog veelal reactief gehandeld.

Voor het opstellen van de richtlijnen kunnen de voorgaande datalekken worden bestudeerd. Aan de hand van die datalekken kunnen de eerste richtlijnen worden opgesteld, waarbij de grootste risico's eerst worden aangepakt.

Ook dient organisatiebreed te worden vastgelegd wanneer een datalek wordt gemeld en wanneer deze enkel intern wordt geregistreerd. Verreweg de meeste datalekken worden tot op heden enkel intern geregistreerd.[60]

Melden van datalekken door derden

Voor derden, zoals studenten, wordt er geen mogelijkheid geboden om een datalek te melden. Het is voor studenten niet duidelijk wat er onder een datalek wordt verstaan én waar zij deze kunnen melden. Tot dusver zijn het veelal studenten met een juridische achtergrond die een datalek weten te melden (en hun rechten uit de AVG uitoefenen).

De meest voor de hand liggende oplossing voor bovenstaande probleem wordt gevonden in het beschikbaar stellen van het Meldpunt Datalekken op de publieke sectie van de RUG-website en een vermelding ervan op te nemen in het Studentenstatuut.

Inventarisatie datalekken

In heel 2018 zijn er **41** beveiligingsincidenten[61] gemeld. Daarvan zijn er **16** als datalek gekwalificeerd en intern geregistreerd, van die 16 datalekken zijn er **4** gemeld bij de Autoriteit Persoonsgegevens en daarvan zijn **3** datalekken gecommuniceerd naar de betrokkenen.

De overige beveiligingsincidenten zijn **1)** niet te kwalificeren als datalek; **2)** is de RUG niet de verantwoordelijke[62] of **3)** worden nog onderzocht.

De datalekken en de adviezen daaromtrent worden momenteel geregistreerd en bijgehouden door de FG. Dit is geen ideale situatie; er moet in 2019 gestreefd worden naar het beheer van datalekken in een gecentraliseerd systeem.

[60] De beoordeling wordt nu enkel gedaan door de Functionaris Gegevensbescherming.
[61] Dit zijn mogelijke datalekken; verder onderzoek bij de RUG wijst uit of een incident ook een datalek is.
[62] Er zijn datalekken gekwalificeerd waarbij UMCG, Lifelines of een studentenvereniging de verantwoordelijke is.

Datalekken in onderzoek

Binnen onderzoek is er afgelopen jaar één datalek geregistreerd. Gezien het grote aantal[63] onderzoeken met persoonsgegevens lijkt dit niet te duiden op excellente beveiliging, maar op gebrek aan kennis over datalekken en de melding daarvan.

Het melden van datalekken is in de onderzoekspraktijk geen onderdeel van de training en/of protocollen. Onderzoekers zijn niet of beperkt bekend met het melden van datalekken.

De RUG dient derhalve te beginnen met de bewustwording van onderzoekers over (het melden van) datalekken.[64] Een logische plek om te starten zijn graduate schools.

[63] Op elk gegeven moment worden er binnen de RUG meer dan 1000 onderzoeken met persoonsgegevens uitgevoerd. Exacte aantallen zijn echter niet bekend vanwege het gebrek aan registratie (zie hiervoor hoofdstuk 6).
[64] Een (korte) training of protocol kan worden opgenomen in het curriculum of aan bod komen bij het datamanagementplan indien er persoonsgegevens bij het onderzoek worden verwerkt.

13. Conclusie

De RUG staat aan het begin van het opzetten van een duurzame privacymanagementorganisatie met de daarbij behorende PDCA-cyclus. Afgelopen jaar stond in het teken van bewustwording en het aanstellen van de juiste mensen op de juiste plekken. Hieronder vallen de ruim 50 privacy- en securitycoördinatoren, maar ook de juristen en beleidsmedewerker. Hierin heeft de RUG een grote stap gezet. Zij zit nu op het volwassenheidsniveau 1,3 voor wat betreft de borging van privacy binnen de organisatie.

Verder heeft de RUG een register in gebruik genomen en tracht het daarmee de doelen en grondslagen van de verwerkingen van persoonsgegevens scherp te krijgen. Binnen onderzoek zijn veel verwerkingen nog niet inzichtelijk waardoor het verbeteren en/of toezichthouden wordt bemoeilijkt, hier moet dit jaar verbetering in komen.

Voor onderzoek dienen de faculteitsbesturen de komende jaren inzet en betrokkenheid te tonen om de beveiliging en de kwaliteit van persoonsgegevens naar een hoger niveau te tillen. De faculteitsbesturen hebben daarbij ondersteuning van centrale diensten nodig om bijvoorbeeld beveiligingsmethodieken als pseudonimisering en encryptie te kunnen implementeren.

Binnen bedrijfsvoering heeft de RUG stappen te maken voor wat betreft de omgang met e-mail, Excel en BYOD. Richtlijnen omtrent zorgvuldige verwerking van persoonsgegevens zijn voor medewerkers in deze fase cruciaal.

Het project BP 2020 en de daaruit voortvloeiende software gaat processen binnen HR en Finance faciliteren. De uiteindelijke inrichting en naleving van de ‘best practices’ bepalen of de nieuwe software bijdraagt aan een zorgvuldigere omgang met persoonsgegevens.

Richting de betrokkenen (studenten, medewerkers en onderzoekssubjecten) zal aankomend jaar meer en duidelijker worden gecommuniceerd over de wijze waarop de RUG met hun persoonsgegevens omgaat. Hieronder valt ook de omgang met datalekken en de mogelijkheden om datalekken te melden.

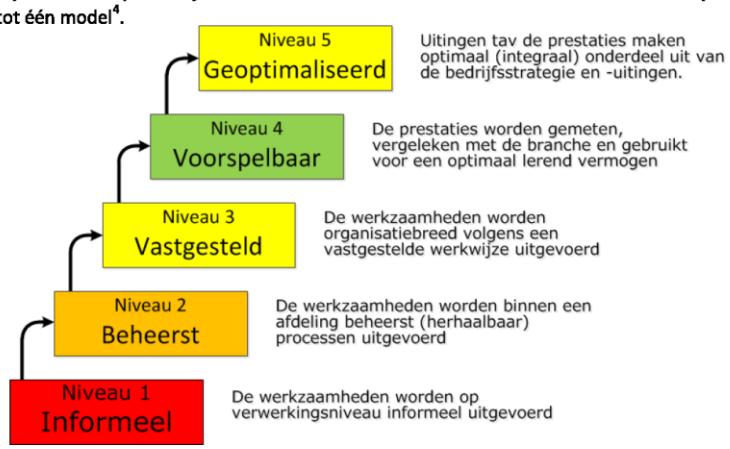
Aan de hand van de interne werkplannen en dit jaarrapport heeft de RUG afdoende handvatten om de borging van privacy binnen de organisatie verder te laten groeien. De FG zal de RUG daarbij adviseren en ondersteunen waar mogelijk. Een ambitieus, maar realistisch streven voor de RUG zou zijn om in 2020 op het volwassenheidsniveau 2,0 te zitten.

Bijlage 1. Privacy Volwassenheidsmodel CIP

2 CMMI en ISOMM vertaald naar het Privacy Volwassenheidsmodel

Het voorliggende Privacy Volwassenheidsmodel onderscheidt vijf niveaus. Ze zijn in paragraaf 1.2 al kort benoemd, hieronder volgt een meer uitgebreide bespreking.

Volwassenheidsmodellen vinden hun oorsprong in het 'Capability Maturity Model' (kort aangeduid als CMM). Het CMM model vindt weer zijn oorsprong in het aangeven van de volwassenheid bij het ontwikkelen van software. Er zijn in de loop der tijd meerdere modellen ontwikkeld. In het CMMI-model zijn modellen geïntegreerd tot één model[4].



Binnen de SIVA methode (ontwikkeld door Wiekram Tewarie) is ook een volwassenheidsmodel beschreven dat wordt aangeduid als 'Information Security Object Maturity level' (ISOMM)[5]. Het voorliggende Privacy Volwassenheidsmodel heeft gebruik gemaakt van CMMI én ISOMM.

CMMI en ISOMM beschrijven volwassenheidsniveaus. De in CMMI en ISOMM gehanteerde niveaus staan nader beschreven in Bijlage 1. Nemen we CMMI en ISOMM als referentie voor de niveaus in het Privacy-volwassenheidsmodel, dan komen we voor de verschillende niveaus tot de vereisten per niveau.
De analyse van CMMI en ISOMM is te vinden in Bijlage 2. Deze analyse heeft geleid tot de onderstaande beschrijvingen van de niveaus waaruit het Privacy volwassenheidsmodel is opgebouwd.

2.1 Niveau 1 – Informeel

Op niveau 1 verzamelt en verwerkt een organisatie persoonsgegevens, waarbij de keuzes per gegevens-verwerking op verwerkingsniveau worden gemaakt vanuit persoonlijk perspectief en afhankelijk zijn van de kennis en kunde van individuele medewerkers. Hierbij ontbreekt het aan formele processen om eisen te stellen aan de verwerking van persoonsgegevens en worden er informeel keuzes gemaakt over hoe er in een concreet geval wordt omgegaan met persoonsgegevens en op welke wijze de gegevens worden verzameld en (verder) verwerkt. Dit betekent dat op dit niveau wel vastlegging kan plaatvinden, maar dat er geen sprake is van vast*stelling*.
Er is geen managementcyclus, waardoor reactief wordt gereageerd op keuzes en incidenten die zich voordoen.

2.2 Niveau 2 – Beheerst proces

Op niveau 2 verzamelt en verwerkt een organisatie persoonsgegevens, waarbij keuzes worden gemaakt op basis van operationeel beleid, richtlijnen en werkinstructies dat door de verwerkingsverantwoordelijken wordt gedeeld en niet meer per gegevensverwerking wordt gepaald.

[4] https://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration#cite_note-Go08-1.
[5] W.N.B. Tewarie, *SIVA, Methodiek voor de ontwikkeling van auditreferentiekaders*, VU University Press, Amsterdam 2014.

Op dit niveau zijn het beleid, de richtlijnen en werkinstructies per afdeling vastgelegd, maar sluiten niet noodzakelijkerwijs aan op de organisatiebrede omgang met persoonsgegevens. Daardoor is de werkwijze op lokaal afdelingsniveau wel traceerbaar, herhaalbaar en gestandaardiseerd, maar nog niet organisatiebreed. *De organisatie leert slechts op lokaal afdelingsniveau*. De verschillende afdelingen kunnen wel van elkaar leren.
Er is wel structurele rapportage over bescherming van gegevens op projectniveau en afdelingsniveau, maar nog geen structurele rapportage van afdelingsniveau naar het hogere management.
Het kan zijn dat er op organisatieniveau wel beleid is, maar dit wordt door de afdelingen niet altijd gehanteerd. Op organisatieniveau kan wel privacybeleid zijn vastgelegd, maar niet officieel bekrachtigd en de controleprocessen om aan dit beleid te voldoen zijn niet organisatiebreed ingericht.

2.3 Niveau 3 – Vastgesteld proces

Op niveau 3 verwerkt een organisatie persoonsgegevens, waarbij keuzes zijn en worden gemaakt op basis van operationeel beleid, richtlijnen en werkinstructies op organisatieniveau. Het beleid is formeel vastgesteld op organisatieniveau en daarmee bekrachtigd als beleid voor de gehele organisatie. De vereisten vanuit de organisatie zijn ook vertaald maar de inrichting van de context, de systemen en de beheerprocessen. *De organisatie leert bedrijfsbreed*, omdat er een systematische samenhang bestaat tussen de uitvoerende onderdelen, beleidsonderdelen en controleonderdelen op zowel afdelingsniveau als bedrijfsniveau. Er is structurele evaluatie van en rapportage over de rechtmatige gegevensverwerking (en beveiliging van persoonsgegevens) naar het hogere management, wat tot aanpassing van het organisatiebrede beleid kan leiden. Er bestaat sturing op de naleving van het beleid, richtlijnen en (werk)instructies. In tegenstelling tot niveau 2 wordt de sturing afgestemd met de bestuurder. De bestuurder is betrokken bij de handhaving van het beleid en de uitvoering, waarbij gerapporteerd wordt ondersteund door controlemiddelen en informatie. Dit leidt tot een lerend proces op zowel afdelingsniveau als op organisatieniveau.

2.4 Niveau 4 – Voorspelbaar proces

Op niveau 4 verzamelt en verwerkt een organisatie persoonsgegevens, waarbij gestuurd wordt op snelheid en kwaliteit van de interacties. De operationele werkelijkheid wordt voortdurend bewaakt en aangepast om de organisatiebrede beleidsdoelen te behalen. Het lerend vermogen in de uitvoerende en specifiek beleidsmatige laag is op niveau 4 tot een maximum *voorspelbaar*.
Het management van de organisatie heeft op ieder gewenst moment inzicht in de stand van zaken omtrent de bescherming van persoonsgegevens in de gegevensverwerkingen en kan die vergelijken met die van de branche. Dit maakt transparantie naar buiten toe mogelijk en de prestatie van de organisatie zichtbaar en meetbaar.

2.5 Niveau 5 – Geoptimaliseerd

Op niveau 5 is er een sterk en expliciet (traceerbaar) verband tussen externe eisen, beveiligingsdoelstellingen, algemeen beleid, specifiek beleid en uitvoering. Aan alle keuzes ligt een uitgebreide, nauwkeurige analyse ten grondslag. Dit resulteert in de mogelijkheid om de organisatie dynamisch aan te passen op basis van praktische ervaringen en prognoses van buiten de eigen organisatie. De operationele werkelijkheid en effectiviteit van beleid worden voortdurend bewaakt. Externe ontwikkelingen, zoals veranderende wet- en regelgeving of maatschappelijke factoren, kunnen snel en soepel worden vertaald naar nieuw specifiek beleid en uitvoering. Bovendien is de organisatie in staat om vooraf prognoses af te geven over kosten en reactiesnelheid. Daardoor zijn weloverwogen keuzes en trefzekere uitkomsten mogelijk. De bewaking en rapportage naar het hogere management is mede gebaseerd op de relatie tussen externe factoren en intern het algemeen beleid, specifiek beleid en de uitvoering. De prestatie-indicatoren zijn eenvoudig traceerbaar en vergelijkbaar met andere organisaties. Het lerend vermogen is op alle lagen tot een maximum geoptimaliseerd, door de verregaande geautomatiseerde feedbacklussen op alle lagen.

