Jaarrapportage bescherming persoonsgegevens RUG 2019

Bewustwording en daadkracht binnen de organisatie groeit

Mr. A.R. Deenen
Functionaris voor de Gegevensbescherming

4 juni 2020

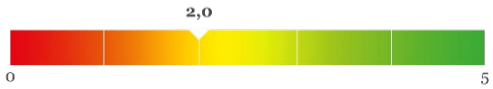
Managementsamenvatting en conclusie

Net als in 2018, is er ook voor 2019 een Jaarrapportage Bescherming Persoonsgegevens RUG 2019 (jaarrapport) geschreven voor het College van Bestuur van de RUG waarin wordt gekeken hoever de RUG is gevorderd in het doorvoeren van de bescherming van persoonsgegevens.

Het doel van dit jaarrapport is om te informeren en te signaleren, maar ook om adviezen te geven en handvatten aan te reiken voor verdere verbetering. Vooral die aspecten met het hoogste risico zullen benoemd worden en bovendien voorzien worden van voorgestelde maatregelen. Verder wordt er in dit jaarrapport teruggekeken naar het afgelopen jaar. Daarbij wordt de vooruitgang en eventuele stagnatie in de ontwikkeling van de privacymanagementorganisatie beschreven. Dit wordt in tien onderwerpen uiteengezet met een bijbehorend volwassenheidsniveau. Het uiteindelijke streven is om voor de RUG een volwassenheidsniveau te behalen van 3,0. Voor 2019 scoort de RUG een 1,7. Dit betekent een verhoging ten opzichte van 2018 (1,3), maar geeft ook aan dat er nog een lange weg te gaan is. Echter, de bewustwording en daadkracht binnen de organisatie en het bestuur groeit. Reden te meer om uit te gaan van een groei in het volwassenheidsniveau voor 2020.

Het volwassenheidsniveau van 1,7 voor 2019 is opgebouwd uit de volgende onderdelen:

Privacybeleid en inbedding in de organisatie:



in overeenstemming met het privacybeleid van de RUG hebben veel faculteiten en diensten werkplannen opgesteld waarin risico's en maatregelen zijn beschreven.

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.

Doelbinding en intern toezicht:

bij de RUG is de controle op de rechtmatigheid en de doelen van alle bestaande en nieuwe verwerkingen van persoonsgegevens nog te beperkt. De FG krijgt wel meer ruimte voor advieswerkzaamheden en toezichthoudende activiteiten, omdat de privacy- en securitycoördinatoren beter gevonden worden en hun kennis gegroeid is.

Register:

het register geeft inzicht en overzicht van de verwerkingen van persoonsgegevens. In 2019 is hiervoor een nieuwe applicatie in gebruik genomen. Bij het vastleggen van nieuwe verwerkingen vindt nu een strengere controle plaats op doel, rechtmatigheid, maatregelen en bewaartermijnen. Inzicht in de verwerkingen binnen het domein onderzoek blijft achter.

Kwaliteitsmanagement:

het niveau van kwaliteitsmanagement binnen de RUG is licht gestegen vanwege de meer structurele borging van de kwaliteit bij nieuw beschreven verwerkingen. Binnen het domein onderzoek wordt de kwaliteit van de persoonsgegevens nog beperkt bewaakt.

Bewaren van persoonsgegevens:

de RUG is op dit onderdeel niet aantoonbaar gegroeid. Naleving van bewaartermijnen en daarmee het verwijderen van persoonsgegevens vindt in geringe mate plaats. Binnen het nieuwe systeem AFAS is integratie met het archief wenselijk.

Beveiligen van persoonsgegevens:

de RUG is gestart met beveiligingsrisicoanalyses en maatregelen worden beschreven en uitgevoerd. Ook beschikt de RUG over een instellingsbreed informatiebeveiligingsplan waarbij de bescherming van persoonsgegevens is meegenomen.

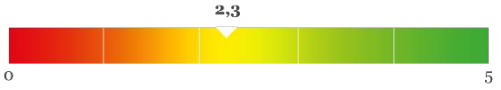
Informatieverstrekking en rechten betrokkenen:

in een hoog tempo werkt de RUG aan de transparantie van de verwerkingen van persoonsgegevens. Hierbij wordt een standaard template gebruikt en een nieuwe compacte versie van de privacyverklaring.

Verwerkersovereenkomsten en doorgifte:

de RUG heeft met het merendeel van de verwerkers afspraken gemaakt. De RUG beschikt over een overzicht dat regelmatig wordt geüpdatet. Controle op de naleving van de verwerkersovereenkomst door verwerkers is zeer beperkt aanwezig.

Datalekken:



Het aantal gemelde datalekken is vergeleken met 2018 vrijwel gelijk gebleven. Wel wordt beter bewaakt dat mitigerende maatregelen naar aanleiding van een datalek daadwerkelijk worden genomen. Binnen het domein onderzoek is meer bewustwording omtrent datalekken gewenst.

Conclusie:

In 2019 heeft de RUG stappen gezet om haar privacymanagementorganisatie verder te laten groeien. Voor een organisatie ter grootte van de RUG, met de drie verschillende domeinen, Bedrijfsvoering, Onderzoek en Onderwijs, en duizenden verwerkingen is dat een nette stap. Dit is te danken aan de inzet van een groot aantal collega’s.

Onder die collega's vallen onder andere de privacy- & securitycoördinatoren. Binnen alle domeinen hebben zij zich verenigd en werken zij toe naar uniforme processen. Dit moet in 2020 resulteren in de groei van het aantal helder omschreven processen in het register. Doelbinding, dataminimalisatie en passende beveiliging moeten binnen die processen op centraal niveau bewaakt worden.
Voor de (ondersteunende) diensten geldt dat zij in 2019 niet geheel aan de verwachtingen voldeden. In 2020 moeten zij aandacht besteden aan hun Werkplannen. Daarin dienen de verwerkingen met de hoogste risico's worden benoemd. Daarnaast is een realistische planning om de risico's te mitigeren vereist. Faculteiten moeten uiteindelijk kunnen vertrouwen op de verwerking van persoonsgegevens in de gefaciliteerde processen en systemen.

Binnen het domein onderzoek is meer aandacht nodig voor de ondersteuning van de onderzoeker. Bewustwording en kennis, maar ook praktische maatregelen zijn nodig. Het vergroten van kennis is ook bij de facultaire ondersteuning en de ethische commissies noodzakelijk.
Naast de interne organisatie, is er meer contact met betrokkenen over de verwerking van hun persoonsgegevens. Het is studenten en medewerkers eenvoudiger gemaakt om persoonsgegevens op te vragen, te rectificeren en te verwijderen. Hierbij speelt een duidelijkere communicatie vanuit de RUG een rol.
Het voornemen om het gemiddelde volwassenheidsniveau op 2,0 te hebben in 2020 is te realiseren. Daarvoor blijft toewijding van het CvB, directies en faculteitsbesturen essentieel.

Indien de RUG in 2020 op het volwassenheidsniveau 2,0 wil zitten, dient de RUG de volgende stappen te nemen:

1. **RUG-breed**
   - diensten en faculteiten stellen realistische en constructieve Werkplannen op;
   - het beheer van autorisaties wordt periodiek gecontroleerd en waar nodig aangepast;
   - vaststellen van richtlijnen rondom het gebruik van persoonlijke e-mailadressen en de verwerking van (bijzondere) persoonsgegevens van betrokkenen;
   - het beveiligingsplan van de RUG deel laten uitmaken van een PDCA-cyclus;
   - stimuleren en bewaken van het gebruik van standaarddocumenten bij het informeren van betrokkenen;
   - structureel bewaken van de naleving van verwerkersovereenkomsten door verwerkers.
2. **Specifiek domein Bedrijfsvoering**
   - nieuwe werknemers een (korte) training laten volgen om zorg te dragen voor een basisniveau aan kennis bij medewerkers;
   - bij processen die leiden tot de inzet van nieuwe applicaties wordt Privacy by Design geïmplementeerd;
   - medewerkers met een bijzondere taak, waaronder de leden van ethische commissies, opleiden in de aspecten van privacy in onderzoek;
   - opstellen van 'Best practices' rond de verwerking van de persoonsgegevens van medewerkers. Deze zijn cruciaal bij de toepassing van AFAS.

3. Specifiek domein Onderwijs

- bewustwording en kennis wordt vergroot bij docenten, onderwijsadministraties en studieadviseurs;
- implementeren van de bewaartermijnen uit de Selectielijst;
- beschrijven en bewaken van uniform beschreven verwerkingen van persoonsgegevens;
- implementeren van (de onderdelen uit het) Project DSD binnen de gehele instelling.

4. Specifiek domein Onderzoek

- kennis bij facultaire onderzoeksondersteuning en ethische commissies wordt vergroot;
- borgen van kennis en kunde bij de centrale onderzoeksondersteuning bij de transitie naar het GDCC;
- technische en organisatorische ondersteuning bieden bij het vormgeven van ‘building blocks’ (sets aan maatregelen);
- het creëren van bewustwording bij onderzoekers over (het melden van) datalekken.

Inhoudsopgave

Verklarende woordenlijst

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

AVG – Algemene Verordening Gegevensbescherming (de officiële Engelstalige afkorting: 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) (*zie AVG*);

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

P&S-coördinator – privacy- en securitycoördinator, aanwezig in elke faculteit en dienst;

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 2019 (“jaarrapport”) voor het College van Bestuur van de RUG. Het jaarrapport is geschreven door de Functionaris voor de Gegevensbescherming (“FG”) van de RUG en heeft dezelfde structuur als het jaarrapport 2018. Het jaarrapport is informerend, signalerend en adviserend van aard.

In het jaarrapport worden de aspecten met het hoogste risico benoemd en de daarbij voorgestelde maatregelen. Het jaarrapport is daarom niet uitputtend bedoeld. Wel is het jaarrapport goed te gebruiken als leidraad voor het aankomende jaar.

Verder wordt in dit jaarrapport teruggekeken naar het voorgaande jaar. Daarbij wordt de vooruitgang en eventuele stagnatie in de ontwikkeling van de privacymanagementorganisatie beschreven.

2. Inleiding

De Algemene Verordening Gegevensbescherming ("AVG") begint na anderhalf jaar steeds meer ingebed te raken. In Nederland zijn de eerste boetes onder de AVG uitgedeeld. De RUG heeft een eerste ronde van werkplannen Privacy & Security achter de rug. Niet onbelangrijk; de intrinsieke motivatie om zorgvuldig met persoonsgegevens om te gaan groeit op alle niveaus.

Na het Project Compliance AVG (2018) en Project Compliance AVG 2.0 (2019) zijn er binnen de domeinen onderwijs, onderzoek en bedrijfsvoering overleggen opgestart tussen de zogenaamde privacy- en securitycoördinatoren ("P&S-coördinatoren"). De P&S-coördinatoren zijn het eerste aanspreekpunt binnen de faculteit of dienst. Daarnaast adviseren zij de directies en faculteitsbesturen bij het opstellen van de werkplannen Privacy & Security ("Werkplannen").

Het Werkplan beschrijft hoe een faculteit of dienst omgaat met de verwerking van persoonsgegevens en hoe zij (hoge) risico's wegneemt bij die verwerking. Het Werkplan is een belangrijk onderdeel binnen de PDCA-cycli in de organisatie.

Ook begint de RUG haar nieuwe verplichtingen te omarmen. Er worden meer *data protection impacts assesments*[1] ("DPIA") uitgevoerd en de resultaten daarvan hebben meer impact dan voorheen. Het nieuwe register is operationeel en dit wordt grondiger gevuld en gecontroleerd door de interne verantwoordelijken en Algemeen Bestuurlijke en Juridische zaken (ABJZ).

Voor studenten is gewerkt aan meer transparantie en is het eenvoudiger gemaakt om rechten uit te oefenen met betrekking tot de eigen persoonsgegevens.

Bij het vaststellen van de volwassenheid van de privacymanagementorganisatie is wederom het model gehanteerd zoals deze door het Centrum Informatiebeveiliging en Privacybescherming is vastgesteld.[2]

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.

Kijkende naar 2019 kan geconcludeerd worden dat het algemene volwassenheidsniveau van de RUG inmiddels op niveau **1,7** ligt. In 2018 bevond de RUG zich nog op niveau 1,3. De

[1] 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."
[2] 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.

inspanning van het afgelopen jaar heeft de eerste vruchten afgeworpen en de verwachting is dat deze stijgende lijn ook voor 2020 doorzet.

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 ().

3. Privacybeleid en inbedding in de organisatie

In lijn met het privacybeleid[3] van de RUG is de borging van privacy en security in 2019 sterk verbeterd. Alle faculteiten en diensten stelden in lijn met het privacybeleid een Werkplan op. Deze zijn door de Security Manager[4] en de FG beoordeeld en zij koppelden terug aan het CvB. Uit de beoordeling blijkt een wisselende voortgang.

De Werkplannen zijn een belangrijke stap geweest bij het inbedden van privacy en security in de (decentrale) organisatie. In de Werkplannen zijn de verantwoordelijkheden binnen de faculteit of dienst beschreven. Ook worden de verwerkingen met de hoogste risico's benoemd en middels een planning toegelicht hoe deze risico's aankomend jaar worden verkleind of weggenomen.

Naast de decentrale besturen en directies dient ook het College van Bestuur zijn bijdrage te leveren. Met de komst van twee nieuwe bestuursleden is de bestuurlijke interesse in privacy en security gegroeid. Op verzoek van het CvB worden processen (meer) geborgd en worden gesprekken gevoerd met alle stakeholders binnen de RUG over de borging van privacy en security.

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.

Borging privacybeleid

De governance inzake privacymanagement is binnen de RUG sinds 2018 vastgelegd in het Algemeen Beleid Bescherming Persoonsgegevens ("privacybeleid"). Dit privacybeleid is in 2019 hernieuwd. De gewenste inhoud van de Werkplannen is verduidelijkt, net als de besluitvormingsprocedure.

[3] Algemeen beleid bescherming persoonsgegevens Rijkuniversiteit Groningen.
[4] De Security Manager bewaakt de algehele IT-beveiliging binnen de RUG en rapporteert daarover aan het CvB.

Het privacybeleid wordt bij de RUG geborgd middels een PDCA-cyclus. Taken en verantwoordelijkheden zijn daarbij beschreven. Vanaf 2019 is bij de implementatie van de PDCA-cyclus afstemming gezocht met de PDCA-cyclus voor de informatiebeveiliging. Dit is een logische stap, want privacy vraagt ook om de toepassing van (technische) beveiligingsmaatregelen.

Wil de RUG de organieke inbedding verder vergroten, dan is de volgende stap het koppelen van de planning aan de benodigde middelen. De Werkplannen 2020 zijn hier de aangewezen plek voor.

Faculteiten en diensten

De faculteitsbesturen en directies van de diensten hebben, ondersteund door de P&S-coördinator(en), in 2019 Werkplannen gepresenteerd met risico's, maatregelen en een planning ten behoeve van een zorgvuldige en veilige verwerking van (persoons)gegevens.

In tegenstelling tot 2018 is de bestuurlijke ondersteuning bij faculteiten en diensten sterker aanwezig. Faculteitsbesturen en directies zijn meer betrokken en meer bewust van de impact en urgentie.

Het merendeel van de Werkplannen 2019 bevat een nette planning van de uit te voeren stappen binnen de faculteit/dienst. Met name de faculteiten hebben constructieve en realistische Werkplannen opgesteld. De Werkplannen zijn beoordeeld door de security manager en de functionaris gegevensbescherming waarbij zij werden ondersteund door ABJZ.

In de onderstaande tabel is de algehele beoordeling ingedeeld in drie categorieën:

(●) goed (●) matig (●) onvoldoende/afwezig

Beoordeling Werkplannen faculteiten			
Faculteit Rechtsgeleerdheid	●	Faculteit Gedrags- en Maatschappijwetenschappen[5]	●/●
Faculteit Economie en Bedrijfskunde	●	Faculteit Campus Fryslân	●
Faculteit Medische Wetenschappen	●	Faculteit Science and Engineering	●
Faculteit Ruimtelijke wetenschappen	●	Faculteit der Letteren	●
Faculteit University College Groningen	●	Faculteit Wijsbegeerte	●
Faculteit Godgeleerdheid en Godsdienstwetenschap	●	Faculteit UMCG onderzoek	●

[5] Ten tijde van de deadline voor de aanlevering van het Werkplan was er geen Werkplan van de Faculteit GMW voorhanden. 17 december heeft de faculteit alsnog een volledig werkplan aangeleverd welke als goed is beoordeeld.

Beoordeling Werkplannen diensten			
Facilitair bedrijf	🟢	Het Bureau	🔴
Centrum voor Informatie Technologie	🔴	Universiteitsbibliotheek	🟢
Talencentrum[6]	🔴		

De vorm en inhoud van de Werkplannen zijn indicatief gebleken voor de daadwerkelijke inzet binnen het veld van privacy en security. Zo zijn datalekken deels te herleiden tot duidelijke risico's die normaliter beschreven worden in het Werkplan en welke daarna gemitigeerd zouden worden (meer over datalekken in hoofdstuk 12).

Voor aankomend jaar is aandacht voor de Werkplannen van de ondersteunende diensten geboden. Zo zijn de Werkplannen van het Bureau en het CIT afgelopen jaar als onvoldoende beoordeeld.

Om als universiteit tot een hoger volwassenheidsniveau te komen, is de medewerking van de diensten onontbeerlijk. Zij leveren een aantal vitale onderdelen voor processen binnen het onderwijs en onderzoek. Ook geven zij de bedrijfsvoering voor het grootste gedeelte vorm. De faculteiten moeten op de diensten kunnen vertrouwen bij het gebruik van de ondersteunde processen en systemen.

De RUG dient derhalve bij de diensten aan te dringen op realistische en constructieve Werkplannen in 2020.

Drie domeinen, drie platformen

Faculteiten hoeven en moeten niet ieder het wiel zelf uitvinden. In gezamenlijkheid is meer te bereiken. Om die reden zijn drie platformen opgezet voor de P&S-coördinatoren: onderwijs, onderzoek en bedrijfsvoering. De 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.

Met de komst van de platformen en Werkplannen worden beslissingen over de toepassing van wettelijke beginselen[7] meer op het niveau van de diensten en faculteiten genomen en in mindere mate op (lokaal) verwerkingsniveau.

Alle faculteiten en praktisch alle diensten hebben op dit moment een of meerdere coördinatoren aangewezen die gefaciliteerd word(t)(en) door het faculteitsbestuur of directie. Dit helpt de RUG te komen tot een hoger volwassenheidsniveau en daarmee tot compliance met de AVG. Per domein volgt hierna de staat van de privacymanagement(organisatie).

[6] Het Talencentrum zou binnen de scope van het Werkplan van de Faculteit der Letteren vallen.
[7] Denk daarbij aan doelbinding, dataminimalisatie, passende beveiliging en transparantie.

Privacy en onderwijs

Met de vaststelling van het beleidsplan Studenten en Onderwijs[8] heeft de RUG een grote stap gezet om de zogenaamde privacybeginselen[9] uit de AVG in de gehele organisatie op een uniforme wijze in te bedden. Het beleidsplan geeft duidelijke handvatten voor de verwerking van persoonsgegevens binnen het domein onderwijs.

Binnen het beleidsplan wordt kort ingegaan op de taken en verantwoordelijkheden. Zo wordt de "proceseigenaar" beschreven als de intern verantwoordelijke die "[..] *dient te waarborgen dat alle medewerkers de verwerking van persoonsgegevens uitvoeren in lijn met het Algemene Beleid Bescherming Persoonsgegevens van de RUG.*"

Het aanwijzen van één proceseigenaar is binnen de RUG voor specifieke verwerkingen niet altijd mogelijk.

Bij meerdere processen is gebleken dat meerdere afdelingen zichzelf aanwijzen als proceseigenaar. Het omgekeerde is binnen de RUG ook mogelijk; geen enkele afdeling ziet zich als dé proceseigenaar van een specifiek proces. Dit betekent dat verantwoordelijkheden niet worden genomen en de zorgvuldige verwerking van persoonsgegevens niet geborgd is.

Taken en verantwoordelijkheden dienen naar aanleiding van het beleidsplan Studenten en Onderwijs verduidelijkt te worden. Daarbij moet nadrukkelijk worden gekeken naar processen waarbij technisch ondersteunende afdelingen de rol van proceseigenaar/-beheerder vervullen.

Docenten en onderwijsadministratie

Binnen het onderwijs zijn het vanzelfsprekend de docenten, het personeel bij de onderwijsadministraties en de studieadviseurs die veelvuldig contact hebben met studenten. In lijn daarmee: het gros van de verwerkingen van persoonsgegevens binnen onderwijs vindt bij hen plaats.

Om de kennis van onderwijzend en ondersteunend personeel te vergroten en beide doelgroepen te faciliteren bij het zorgvuldig verwerken van persoonsgegevens is verdere bewustwording gewenst.

Met als doel dat de medewerker in kwestie kan signaleren wanneer hij/zij de P&S-coördinator moet benaderen en daarnaast de Privacy Portal kan gebruiken.

[8] Beleidsplan Domein Studenten en Onderwijs: Beleid en richtlijnen voor de zorgvuldige verwerking van persoonsgegevens, geschreven in 2019 en door het CvB vastgesteld op 14 januari 2020.
[9] De privacybeginselen worden gevonden in artikel 5 AVG.

Verwerking persoonsgegevens door studenten

Op het snijvlak tussen de domeinen onderwijs en onderzoek bevindt zich het onderzoek dat studenten uitvoeren binnen het curriculum van de opleiding. Hierbij kan gedacht worden aan onderzoek ten behoeve van een scriptie en opdrachten binnen vakken in de bachelor- en masterfase.

Het onderzoek dat tijdens de studie plaatsvindt kent veelal geen ethische toetsing of een verplicht datamanagementplan. Desondanks is de RUG vaak wel de verantwoordelijke.

Studenten die onderzoek doen met persoonsgegevens zijn doorgaans niet bewust van de noodzakelijke technische en organisatorische maatregelen die nodig zijn om persoonsgegevens zorgvuldig te verwerken.[10]

Om te komen tot zorgvuldige verwerkingen van persoonsgegevens door de student, is het vergroten van bewustwording en kennis nodig. Dit dient plaats te vinden voorafgaand aan de verwerking van persoonsgegevens binnen onderzoek.

Relevant en bruikbaar materiaal voor bewustwording en training heeft de RUG reeds in huis in de vorm van de e-learning “Privacy in research: asking the right questions”.[11]

Onderzoek en persoonsgegevens

De RUG kent een groot portfolio aan onderzoeken met persoonsgegevens. Binnen het onderzoeksveld zijn taken, verantwoordelijkheden en bevoegdheden nog onduidelijk.

Het begint met de onderzoeker. De onderzoeker heeft een belangrijke verantwoordelijkheid voor de verwerking van de data (lees: persoonsgegevens). De onderzoeker dient kennis te hebben van de beginselen uit de AVG. De implementatie van die beginselen vraagt namelijk om de toepassing van technische en organisatorische maatregelen.

Zoals ook in het privacybeleid is geformuleerd gaat het bij onderzoek om een gedeelde verantwoordelijkheid. Op centraal en decentraal niveau dient verantwoord onderzoek te worden gefaciliteerd met bijvoorbeeld richtlijnen omtrent de invulling van de beginselen.

De wijze waarop ondersteuning van deze onderzoeken en onderzoekers vorm moet krijgen is niet centraal vastgelegd. De inrichting en het kennisniveau lopen binnen de faculteiten en ondersteunende diensten dan ook sterk uit elkaar.[12]

Ook de rol van de ethische commissie bij de toetsing op de beginselen van de AVG is niet

[10] Zoals afgelopen jaar is gebleken kan de verwerking van persoonsgegevens door studenten leiden tot een datalek.
[11] De e-learning is terug te vinden op de website van de RUG: https://www.rug.nl/research/research-data-management/data_protection-gdpr/data_protection/training-privacy-in-research.
[12] Het werkproces bij de Faculteit GMW vormt een goed voorbeeld voor de overige faculteiten die onderzoek met persoonsgegevens doen. De onderzoeker doorloopt namelijk een vast stramien bij ethische toetsing (EC Request).

geconcretiseerd. De ethische commissies die de AVG-beginselen wel meenemen in de (ethische) toetsing bezitten niet altijd voldoende kennis om effectief te toetsen.[13]

Om de onderzoeker voldoende te kunnen ondersteunen is degelijke inrichting en kennis bij de facultaire onderzoeksondersteuning noodzakelijk.[14] Periodieke training van het ondersteunend personeel is daarom gewenst. Dit geldt tevens voor de leden van de ethische commissies.

Vanuit de centrale organisatie levert het Research Data Office ("RDO") ondersteuning aan onderzoekers die vragen hebben over (de toepassing) van persoonsgegevens. Bij het RDO zijn derhalve relevante kennis en bruikbare 'best practices' aanwezig.

De inrichting en kennis bij de centrale organisatie is echter nog niet geborgd. Wat die organisatie betreft, de universiteit lijkt haar derde transitie in een korte periode te ondergaan.[15] RDO en de Data Federation Hub (DFH)[16] zullen hoogstwaarschijnlijk niet langer blijven bestaan. Dit en het achterwege blijven van structurele plannen voor de inrichting van het RDO resulteerde in 2019/2020 al tot het wegvloeien van essentiële expertise. In de plaats van RDO/DFH wordt het Groningen Digital Competence Center ("GDCC") opgericht. De overheid stimuleert (financieel) de opzet van DCC's in Nederland.[17]

Met de oprichting van het GDCC ligt de focus op (lokale) data stewards en de stimulering van interuniversitaire DCC's bij uitwisseling en dataopslag volgens de FAIR-principes[18].

Die steun ziet met name op de ICT-infrastructuur en de ondersteuning daarvan. Onderzoeksbegeleiding dient in eerste instantie geen techniekgedreven exercitie te zijn. Techniek is immers op zich geen doel, maar een (belangrijk) middel bij onderzoek.

Bij de inrichting van het GDCC dienen privacy en security bij alle onderdelen nevengeschikt (dus niet ondergeschikt) te zijn. Privacy is meer dan een randverschijnsel bij Open Science. Ook dient de huidige kennis en expertise geborgd te worden.

Research Datamanagementplannen

Naast de inrichting van het GDCC en de inzet van data stewards, is effectieve ondersteuning bijna niet mogelijk zonder het gebruik van research data management plannen ("RDMP"). Aan de hand van een RDMP kan gezocht worden naar én geadviseerd worden over passende maatregelen om risico's te verkleinen of weg te nemen vóór, tijdens en na het onderzoek.

Sinds 2015 wordt met het RUG Research Databeleid aangedrongen op de toepassing van RDMP. Het onderzoeksinstituut of de faculteit dient de kaders daarvoor aan te dragen. Bij een

[13] Het kan hierbij gaan om basale kennis over definities als "persoonsgegevens" of "pseudonimisering".
[14] Wetenschap over bestaande 'building blocks' valt hier ook onder. Meer over building blocks in hoofdstuk 9.
[15] Tussen 2013-2016 stond het RDO centraal en van 2016-2018 was dat het programma Human Subject Research.
[16] DFH verbindt verschillende initiatieven op het gebied van research data bij RUG en UMCG met elkaar.
[17] Zie ook het Uitvoeringsplan investeringen digitale onderzoeksinfrastructuur (1 oktober 2019) van de NWO.
[18] FAIR staat voor "to be Findable", "to be Accessible", "to be Interoperable" en "to be re-usable".

groot aantal faculteiten is het RDMP onderdeel van het werkproces van de onderzoeker. Een kleiner deel van de faculteiten maakt echter geen of beperkt gebruik van RDMP.[19]

Zorg op centraal niveau voor goede ondersteuning van de instituten en daarmee de onderzoekers.[20] Dit geldt voor alle faculteiten. Naast compliance met de AVG kunnen ook de zorgplichten uit de Gedragscode Wetenschappelijke Integriteit ("Gedragscode WI") op die manier beter worden ingevuld.

Bedrijfsvoering en persoonsgegevens

Alle circa 6.000 medewerkers bij de RUG verwerken op de een of andere wijze persoonsgegevens. Zorgvuldige verwerking begint bij het gebruik van het gezonde verstand van die medewerkers.

Om zorgvuldig met persoonsgegevens om te gaan hoeft eenieder geen privacyprofessional te zijn. Grofweg de kaders kennen van de AVG en derhalve kunnen signaleren wanneer een P&S-coördinator moet worden ingeschakeld, is wel essentieel om te kunnen groeien in de volwassenheid van de privacymanagementorganisatie.

Bij de indiensttreding wordt gebruikgemaakt van zogenaamde "onboarding". Om structureel kennis binnen de organisatie te vergroten is toevoeging van de Workshop Data en Privacy (AVG) aan de onboarding zeer wenselijk.

Naast nieuwe medewerkers vertrekken er ook continu medewerkers. Deze medewerkers hebben rollen en rechten in meerdere systemen en beheren vaak veel persoonsgegevens op (persoonlijke) apparatuur en e-mailaccounts. Voor medewerkers die een andere functie binnen de RUG gaan bekleden geldt hetzelfde.

De controle op het tijdig ontnemen van rollen en rechten is summier en wordt niet altijd standaard volledig uitgevoerd. Dit geldt tevens voor (uitgeleende) apparatuur en de persoonsgegevens die daarop staan. Dergelijke situaties leiden al snel tot datalekken.

Voor (grote) systemen en schijven dient de RUG bij vertrek of wisseling van functie van een medewerker de rollen/rechten zoveel mogelijk te ontnemen om indien nodig daarna zorgvuldig op te bouwen. Het creëren van een protocol of het aanwijzen van een verantwoordelijke centrale organisatie kan daarbij zinvol zijn.

Bovenstaande risico's worden grotendeels gemitigeerd met de inbedding van privacymanagement binnen het Bureau en CIT. Meer over risicomanagement binnen de diensten in hoofdstuk 4.

[19] Deze uitkomsten volgen uit de Research Data Management Audit 2018-2019 bij de RUG.
[20] Hierbij kan gedacht worden aan het trainen van ondersteunend personeel, zoals data stewards.

Informatiemanagement en -beveiliging

Naast kennis en bewustwording ten aanzien van de AVG, is op centraal niveau meer regie vereist op informatiemanagement en –beveiliging.

Binnen de RUG is er geen centrale entiteit die in kader van de informatiestromen kan adviseren en strategie uitzet. Informatiemanagement is grotendeels ondergebracht bij het CIT. CIT lijkt daardoor vraag en aanbod te beheren. Dit leidt niet per se tot de meest wenselijke oplossingen voor de RUG als geheel.

Hetzelfde geldt voor toezicht op de informatiebeveiliging. De RUG heeft in 2019 geen Chief Information Security Officer (CISO) aangewezen. Wel heeft de RUG een security manager die ondergebracht is bij het CIT. Informatiebeveiliging en het toezicht daarop is derhalve ondergebracht bij het CIT.

Indien de RUG ervoor kiest om de functie van CISO in te laten vullen door de security manager, dient de inbedding van deze persoon gewijzigd te worden. De CISO schrijft namelijk beleid en risicogebaseerde prioriteiten die deels door het CIT vertaald en uitgevoerd dient te worden. Ook behandelt hij incidenten die hun oorsprong vinden bij het CIT. Dit maakt dat de CISO onafhankelijk van de IT-directeur moet kunnen functioneren.[21]

Concluderend

Met de beschreven stappen concretiseert de RUG de privacywet- en regelgeving op een eenduidige en formele wijze in (privacy)beleid.

Beslissingen over de toepassing van beginselen[22] uit de privacywetgeving worden meer op het niveau van faculteiten en diensten genomen. Dit betekent dat beslissingen over de toepassing van de beginselen steeds minder bij de individuen (op verwerkingsniveau) liggen.

Naast het beleid, is de organieke inbedding van taken en verantwoordelijkheden verbeterd. Op decentraal niveau zijn deze zaken helderder beschreven en vastgelegd.

Het streven van de RUG zal moeten zijn om op centraal niveau voor de gehele organisatie de taken, verantwoordelijkheden en bevoegdheden te beschrijven en formeel vast te leggen. Van veel omvangrijke en faculteitoverstijgende verwerkingen is dit niet (formeel) vastgelegd.[23]

Om in 2020 verder te groeien op dit onderdeel, is in beginsel extra aandacht voor het domein onderzoek nodig. Hier is veel laaghangend fruit aanwezig.

---

[21] Position Paper: Inrichting governance van cybersecurity in het hoger onderwijs. Pas toe of leg uit!, Platform Integrale Veiligheid Hoger Onderwijs / KPMG, 20 april 2020.

[22] Hieronder vallen onder meer “dataminimalisatie”, “doelbinding”, “opslagbeperking” en “transparantie”.

[23] Denk aan de governance omtrent rollen en rechten in AFAS of de verantwoordelijkheden binnen onderwijssystemen als Progress.

4. Risicomanagement

De AVG vraagt om een risicogedreven aanpak. De bescherming van persoonsgegevens bestaat deels uit het wegnemen van risico's. Niet alle risico's zijn even groot of urgent. De Werkplannen van de faculteiten en diensten leveren inzicht in de aanwezige risico's. Het inzicht is echter nog beperkt.

Om risicogedreven te werk te gaan binnen de RUG is een inventarisatie van de risico's onontbeerlijk. Dit is echter eerste stap. Na de inventarisatie dient afhankelijk van de hoogte van het risico gepast te worden gehandeld. In het afgelopen jaar is weinig groei geconstateerd voor de universiteit op dit onderdeel. Daarbij speelt mee dat niet alle Werkplannen zijn opgeleverd en veel Werkplannen de (hoge) risico's niet benoemen.

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.

Goede voorbeelden van Werkplannen zijn onder meer die van de Universiteitsbibliotheek, de Faculteit Rechtsgeleerdheid en de Faculteit Economie en Bedrijfskunde.

Die kwaliteit geldt niet voor alle diensten en faculteiten. Belangrijke entiteiten binnen de RUG als het Bureau en het CIT hebben deze exercitie onvoldoende uitgevoerd (zie hoofdstuk 3). Dergelijke interne dienstverleners vormen echter wel de ruggengraat voor de informatiebeheersing binnen de RUG.

Zij dienen de risico's te beschrijven en daarbij rekening te houden met de interne afnemers. Derhalve niet reactief handelen, maar proactief werken. Interne afnemers als faculteiten hebben zelfstandig namelijk niet het overzicht en inzicht om te bepalen wat de risico's zijn van verwerkingen die door het CIT of Bureau worden gefaciliteerd.

Het in kaart brengen en beoordelen van risico's zijn onderdelen waar de RUG veel winst kan behalen. Zo zijn DPIA's (risico-inventarisatie) geen onderdeel van bedrijfsprocessen. DPIA's worden binnen de domeinen bedrijfsvoering en onderwijs onder meer uitgevoerd op aanwijzen van ABJZ. Binnen onderzoek wordt een DPIA uitgevoerd nadat RDO dit aan een onderzoeker of onderzoeksgroep heeft geadviseerd.

Binnen alle domeinen is de DPIA nog een vrij onbekend fenomeen. Kennis bij het algehele personeel over het uitvoeren van een DPIA is niet nodig. Het instrueren van projectmanagers en relevante spelers bij het initiëren van nieuwe verwerkingen daarentegen wel.

Verder worden de meeste DPIA's uitgevoerd op decentraal niveau en zijn slechts beperkt inzichtelijk binnen de rest van de organisatie. Uitkomsten en betekenis worden derhalve niet vergeleken en niet op organisatieniveau vastgesteld. Dit resulteert in het informeel vaststellen van passende maatregelen en worden risico's op een inefficiënte wijze gemitigeerd.

Privacy by design

Een andere wijze om risico's te beperken is te vinden in het (wettelijk vastgelegde) beginsel van "privacy by design"[24]. Dit omvat het betrekken van privacy en security bij de vormgeving van processen en systemen.

Privacy by design dient terug te komen bij de uitvraag van diensten en producten (lees: aanbestedingen), maar ook bij de (interne) ontwikkeling van processen en applicaties.

Privacy by Design dient aan bod te komen bij de ontwikkeling of uitvraag van nieuwe applicaties/diensten. Het zal derhalve ingebed moeten worden bij de relevante processen binnen het CIT en het Facilitair Bedrijf.

Beheer informatie en applicaties

Het IT-landschap bij de RUG is bijzonder. Nieuwe applicaties schieten als paddenstoelen uit de grond. Deze worden aangekocht of door de RUG ontwikkeld. Dit gebeurt praktisch op alle niveaus binnen de RUG. Zolang beheer plaatsvindt en duidelijk is wat er binnen welk proces en applicatie afspeelt is de RUG "in control". Dit is echter al enige tijd niet zo.

Binnen de RUG zijn verschillende systemen/applicaties zogenaamd "end of life". Wat zoveel betekent dat ze niet meer worden geüpdatet en/of ondersteund. Intern betekent dat dat de kennis en/of de middelen niet meer beschikbaar zijn. Extern kan dat betekenen dat de leverancier de software niet meer updatet.

Om dergelijke onnodige risico's te beperken is het belangrijk dat de RUG grip krijgt op de introductie van nieuwe applicaties. Om dit doel te bereiken en te borgen dat de RUG voor één doel niet meerdere applicaties opneemt in haar IT-portfolio, is RUG Information Office (RIO) in het leven geroepen.

RIO helpt de organisatie om de huidige situatie scherp te krijgen en voor de gewenste situatie de eisen ten aanzien van de oplossing duidelijk te specificeren. Dit omvat meer dan gebruikerseisen. De uitgangspunten van ICT- en businessarchitectuur, beveiliging en

[24] De autoriteit op dit gebied is de universitair hoofddocent dr. J.H. Hoepman, werkzaam bij de RUG en auteur van het boek over privacy by design: Hoepman, J.-H., Privacyontwerpstrategieën (Het Blauwe Boekje), Nijmegen: Radboud Universiteit 2018.

wettelijke vereisten worden meegenomen. Hierbij wordt rekening gehouden met het totale applicatielandschap en levenscyclus van applicaties. RIO borgt zo onder meer: 1) de inzet van bestaande applicaties voor nieuwe processen en; 2) dat er zoveel mogelijk privacy-by-design wordt gewerkt en afspraken contractueel vastliggen.

De afdeling RIO dient ingebed te worden in de organisatie en vast onderdeel te worden van de werkprocessen die leiden tot nieuwe applicaties en toepassingen.

Risico-inventarisatie WhatsApp

In oktober en november van het afgelopen jaar is er een DPIA uitgevoerd op zogenaamde messaging applicaties (apps). De bevindingen daarvan zijn direct toegepast in hetzelfde DPIA op een van de meest gebruikte messaging apps: WhatsApp. De resultaten zijn op 12 december gepubliceerd. Daaruit blijkt dat er grote uitdagingen bestaan bij gebruik van messaging apps en in het bijzonder WhatsApp binnen de bedrijfsvoering van de RUG.

De belangrijkste bevindingen zijn:

1. duidelijke vereisten voor de leverancier en de technologie ontbreken binnen de RUG;
2. er is geen beleid omtrent gebruik van messaging apps door personeel;
3. medewerkers hebben geen reëel beeld van de risico's wanneer zij deze apps gebruiken;
4. beginselen uit de AVG worden veelal niet nageleefd wanneer WhatsApp wordt gehanteerd binnen de bedrijfsvoering.[25]

Dit zijn lastige bevindingen, omdat het gaat om apps die in veel gevallen de kern vormen van alle (informele) communicatie binnen de RUG. Ondanks dat WhatsApp en overige messaging apps onderdeel uitmaken van ons dagelijks leven, kan de RUG wel degelijk een aantal risico's mitigeren. En dat zonder buitenproportionele krachtsinspanning.

Formuleer eisen voor het gebruik van messaging apps en de leveranciers welke zijn gebaseerd op de uitkomsten van de DPIA. Hierna kan het fundament gelegd worden in de vorm van beleid omtrent het gebruik van messaging apps. Ook is het van belang om personeel te wijzen op goed ingerichte alternatieven alvorens specifieke apps te ontmoedigen.

Onderzoek(ers)

Ten opzichte van het voorgaande jaar vonden er weinig relevante wijzigingen plaats binnen het domein onderzoek. Er worden nog steeds duizenden wetenschappelijke onderzoeken uitgevoerd waarbij een deel persoonsgegevens verwerkt.

[25] In het geval van WhatsApp kan gedacht worden aan strijd met de volgende beginselen: rechtmatigheid, dataminimalisatie, opslagbeperking, transparantie en beveiliging.

Het exacte aantal onderzoeken met persoonsgegevens, hoe deze onderzoeken worden uitgevoerd en waar het onderzoek plaatsvindt is grotendeels onbekend.[26] De RUG kan derhalve niet voldoen aan haar verantwoordingsplicht. Het gevolg is ook dat de RUG niet kan garanderen dat bij alle onderzoeken passende technische en organisatorische maatregelen worden getroffen.

Het vergroten van kennis bij de onderzoeker en de inzet van RDMP brengt het onderzoek en de daarbij behorende risico's eerder in kaart. Zie hiervoor hoofdstuk 3.

[26] Meer hierover in hoofdstuk 6. Register.

5. Doelbinding en intern toezicht

Bij de verwerking van persoonsgegevens is het doel onmisbaar. Welke gegevens de RUG precies nodig heeft voor de verwerking is hiervan afhankelijk. Daarnaast is voor elke verwerking van persoonsgegevens een zogenaamde grondslag nodig. Vastleggen van doelen en grondslagen op centraal niveau maakt effectieve controle voor de functionaris gegevensbescherming mogelijk.

Momenteel worden de doelen nog informeel[27] bepaald en kent de RUG nog onvoldoende uniformering op dit vlak. Dit resulteert in gelijksoortige verwerkingen waarbij de doelen uiteenlopen. Doelen liggen derhalve niet altijd in lijn met de gecommuniceerde doelen.

In de Algemene privacyverklaring Rijksuniversiteit Groningen ("privacyverklaring") zijn wel globaal de doelen van de verwerkingen bij de RUG vastgelegd. Dit maakt effectieve controle op doelbinding[28] echter nog niet mogelijk. De uniformiteit is binnen de verwerkingen beperkt aanwezig is en derhalve zouden dan vele duizenden individuele verwerkingen periodiek gecontroleerd moeten worden.

Effectieve controle op de doelen van verwerkingen kan worden bereikt door zoveel mogelijk op centraal niveau doelen en grondslagen van verwerkingen vast te stellen. Daarbij dienen de instellingsbrede doelen te worden gekoppeld aan gestandaardiseerde processen binnen de RUG.

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[29] hebben voor de organisatie zelf.

[27] Dit betekent dat (individuele) medewerkers die persoonsgegevens verwerken bepalen voor welke doelen de persoonsgegevens worden ingezet. De RUG heeft hier dan geen of minimale controle over.
[28] Doelbinding houdt in dat persoonsgegevens niet nog voor andere (onverenigbare) doelen worden ingezet dan de doelen waarvoor ze initieel zijn verzameld.
[29] Hierbij moet gedacht worden aan bestuurlijke boetes, imagoschade of verlies van vertrouwen door stakeholders.

Uniforme doelen na 2019

Sinds het voorgaande jaar zijn er plannen gemaakt om toe te werken naar uniform beschreven doelen en de vastlegging daarvan.[30] Naar verwachting wordt er in 2020 goede voortgang geboekt met het formuleren en vaststellen van uniforme doelen binnen de RUG. De RUG heeft in februari 2020 Projectplan Privacy & Security goedgekeurd. Dit projectplan bevat ruimte voor een medewerker om de actualiteit, uniformiteit en volledigheid van het register te borgen. De doelen worden derhalve vastgelegd in het register.

Met de hantering van uniform vastgelegde doelen, wordt het eenvoudiger om te toetsen of persoonsgegevens noodzakelijk zijn bij specifieke verwerkingen. Ook wordt het eenvoudiger om op centraal niveau de volgende aspecten te controleren: de volledigheid, de juistheid en de bewaartermijnen.

Het controleren en daarmee het toezicht houden op het rechtmatig verwerken van persoonsgegevens is neergelegd bij de faculteitsbesturen en directies. Het algemene interne toezicht wordt ingevuld door de FG.

Intern toezicht

Binnen de RUG ziet de FG toe op alle processen, beleid en maatregelen omtrent de verwerking van persoonsgegevens. Daarbij werkt de FG samen met de privacysectie van ABJZ en de P&S-coördinatoren van alle domeinen. Ook heeft de FG korte lijnen met de security managers.

In 2019 is een aantal nieuwe Privacy- en Securitycoördinatoren (“P&S-coördinatoren”) aangesteld. De nieuw aangestelde P&S-coördinatoren zijn in de regel toegewijd en deskundig. Dit zorgt er op zijn beurt voor dat de FG meer focus heeft op zijn adviserend en toezichthoudend werk.

Zoals uit deze jaarrapportage blijkt, is de groei van het volwassenheidsniveau van het privacymanagement zichtbaar. Dit is echter nog niet dusdanig dat dit resulteert in een afname van de werkzaamheden van de FG.

De FG komt in 2019 niet toe aan het uitoefenen van zijn wettelijke taken. Zo is het praktisch onmogelijk gebleken om toe te zien op alle audits. Ook is het niet mogelijk om tijdig alle uitgevoerde DPIA’s te beoordelen en van advies te voorzien.[31]

Naast de wettelijke taken, beoordeelt de FG binnen de RUG alle inbreuken op de bescherming van persoonsgegevens (“datalekken”). Hierover adviseert hij het CvB. De FG hanteert meerdere gradaties van risicoprofielen bij datalekken. De datalekken met een middel of hoog

[30] In hoofdstuk 6 Register worden de uniforme processen verder uiteengezet.
[31] In het geval van Europese subsidieverstrekkers kan de beoordeling van de FG binnen een DPIA cruciaal zijn voor de daadwerkelijke verstrekking van gelden voor onderzoek.

risicoprofiel hebben prioriteit.[32] Advisering omtrent datalekken met een laag risicoprofiel laten in sommige gevallen enkele weken op zich wachten.[33] Dit is niet wenselijk.

[32] Datalekken met een middel of hoog risicoprofiel worden gemeld bij de Autoriteit Persoonsgegevens (“AP”) respectievelijk de AP en de betrokkenen.
[33] Datalekken met een laag risicoprofiel worden enkel intern gedocumenteerd.

6. Register

Het in kaart hebben van de verwerkingen met persoonsgegevens is wat de AVG vereist. Dit wordt het register van verwerkingsactiviteiten genoemd (“register”). Met het register toont de RUG aan dat zij voldoet aan de regelgeving rond de zorgvuldige verwerking van persoonsgegevens. Op verzoek van de Autoriteit Persoonsgegevens (“AP”) dient de RUG dit register te kunnen overdragen.

In technische zin heeft de RUG in 2019 een flinke stap gezet. De registertool *Privacy Perfect* is binnen de domeinen bedrijfsvoering en onderwijs in gebruik genomen. Nieuwe verwerkingen worden voor die domeinen niet meer in de zogenaamde Research Data Management Plan-tool (“RDMP-tool”) beschreven.

Verwerkingen binnen het domein onderzoek vinden plaats in de RDMP-tool of in applicaties die de gegevens kunnen doorzetten naar de RDMP-tool.

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.[34]

Met het in gebruik nemen van Privacy Perfect vindt er een strengere controle aan de poort plaats. Het uitgangspunt is nu: P&S-coördinatoren beschrijven gezamenlijk met de leden van het privacyteam (ABJZ) de verwerkingen. Zoals de verwerking is beschreven dient deze centraal en decentraal uitgevoerd te worden. Op die manier worden technische en organisatorische maatregelen, maar ook doelen[35] op een organisatiebrede wijze bepaald.

De andere registertool, de RDMP-tool, kent circa 2.000 beschreven verwerkingen. Privacy Perfect bevat op het moment van schrijven 60 verwerkingen. Voordat alle verwerkingen helder zijn beschreven in Privacy Perfect, zijn we minimaal twee jaar verder. Dit is onoverkomelijk, omdat de decentrale eenheden veelal overeenstemming moet bereiken over de invulling van

[34] Een verplichting daartoe is te vinden in art. 30 lid 4 AVG.
[35] Zie hiervoor ook hoofdstuk 5 over doelbinding bij de RUG.

vele verwerkingen. Dit is deels een bottom-up exercitie, omdat personeel op de werkvloer in de praktijk weet hoe een verwerking (op een werkbare wijze) vorm kan krijgen.

Aansluitend wordt er bij het beschrijven van verwerkingen in het register ook direct gekeken naar de transparantie richting betrokkenen. Met andere woorden, hoe leg je een student of medewerker helder uit wat je met hun (persoons)gegevens doet en met welk doel. Dit wordt verder beschreven in hoofdstuk 10 Informatieverstrekking en rechten betrokkenen.

Op dit moment heeft de RUG op centraal niveau nog niet een compleet en actueel beeld van alle verwerkingen van persoonsgegevens. Dit is vanuit het perspectief van de bescherming van de “rechten en vrijheden” van de betrokkenen niet onoverkomelijk, zolang op decentraal niveau zicht is op alle verwerkingen. Dit laatste is echter nog niet het geval. Door de bank genomen zijn faculteiten beter in staat om een zorgvuldige omgang te bewerkstelligen.

Belangrijk is om op decentraal niveau te komen tot een zorgvuldige verwerking van persoonsgegevens.[36] Het vullen van het register met de uniform beschreven verwerkingen is het uitgangspunt binnen de domeinen bedrijfsvoering en onderwijs.

Onderzoek met persoonsgegevens deels in beeld

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 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. Met enkel de RDMP-tool voldoet de RUG nog niet aan alle vereisten wanneer het wetenschappelijke onderzoek betreft 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.[37]

De faculteiten zijn verantwoordelijk voor onderzoek en de inventarisatie van onderzoeken. Zij dienen (evt.) in samenspraak met RDO in het Werkplan maatregelen te beschrijven om te komen tot een volledig overzicht van verwerkingen in onderzoek.

[36] Bij een zorgvuldige verwerking worden beginselen als transparantie, dataminimalisatie, opslagbeperking, integriteit en vertrouwelijkheid meegenomen.
[37] Zie hiervoor ook de opmerkingen in hoofdstuk 4 onder “Onderzoek(ers)”.

Verder bevat de RDMP-tool nog niet voor alle beschreven verwerkingen de bewaartermijnen en omschrijving van de technische en organisatorische beveiligingsmaatregelen.

In 2020 dient op centraal niveau bepaald te worden wie verantwoordelijk is voor de kaders om wel te komen tot volledig beschreven verwerkingen.
Het advies is om op decentraal niveau gestandaardiseerde processen[38] vast te stellen die in beginsel moeten worden gevolgd binnen de desbetreffende faculteit. Bij de vormgeving van deze processen wordt een minimum aan beveiligingsmaatregelen en de maximale bewaartermijnen omschreven.

Gezamenlijk register RUG-UMCG

Binnen alle domeinen vindt er samenwerking plaatst tussen de RUG en het UMCG. Afspraken over deze samenwerking zijn beschreven in een Raamovereenkomst. Eén van de afspraken behelst het opzetten en onderhouden van een gezamenlijk register.

In 2019 zijn partijen meerdere malen bij elkaar gekomen om de gezamenlijke verwerkingen binnen de domeinen bedrijfsvoering en onderwijs in kaart te brengen. Het gros van deze verwerkingen is in kaart gebracht en beschreven. Daarbij is ook verduidelijkt welke partij welke rol en verantwoordelijkheden heeft.

Het gezamenlijke register omvat niet de verwerkingen binnen het domein onderzoek.

Het in kaart brengen van verwerkingen binnen het domein onderzoek zal een uitdaging zijn in 2020/2021. Het beschrijven an sich vormt geen uitdaging voor de RUG, maar het achterhalen van lopende en afgeronde onderzoeken is lastig. Temeer nu de RUG nog maar een deel van de onderzoeken met persoonsgegevens in kaart heeft gebracht, dan wel waarneemt.

De RUG dient afspraken te maken met het UMCG over het structureel in kaart brengen en beschrijven van verwerkingen van persoonsgegevens binnen het onderzoeksveld.

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.[39]

[38] De gestandaardiseerde processen worden gebaseerd op de thans geregistreerde verwerkingen. Deze processen worden elders binnen de RUG ook wel beschreven als “onderzoekscenario’s”.
[39] Dit sluit aan bij de bevindingen over het beheer op de verwerkersovereenkomsten in hoofdstuk 11.

7. Kwaliteitsmanagement

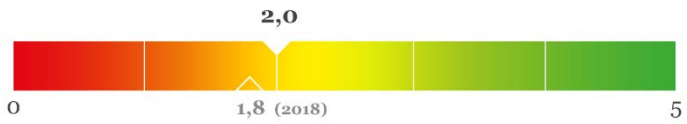
De kwaliteit van persoonsgegevens en de processen die dat borgen is waar kwaliteitsmanagement over gaat. Hieronder valt het bewaken van de nauwkeurigheid en juistheid van persoonsgegevens. Ook valt hieronder het kunnen rectificeren, vervolledigen, verwijderen en beperken van de verwerking van persoonsgegevens wanneer persoonsgegevens niet juist of onnauwkeurig zijn.

Het niveau van kwaliteitsmanagement is binnen de RUG licht gestegen.[40] Wel is er een verschil waar te nemen binnen de drie domeinen en daarmee een verschil per categorie betrokkenen wiens persoonsgegevens het betreffen. De drie belangrijkste categorieën zijn studenten, medewerkers en deelnemers bij onderzoek ("onderzoekssubjecten").

De lichte stijging in het volwassenheidsniveau is te verklaren door de structurele inzet en bewaking van privacyverklaringen. Een privacyverklaring beschrijft waarom en hoe de RUG binnen een verwerking met persoonsgegevens omgaat. Het is daarom aan de RUG om dit document helder en bondig vormt te geven. De RUG heeft getracht met een compact en visueler document studenten, medewerkers en overige betrokkenen te informeren. In Bijlage 2. Compact model privacyverklaring RUG vindt men een voorbeeld.

Voor nieuwe verwerkingen die in het register (hoofdstuk 6) worden geplaatst, wordt gekeken naar de informatieverstrekking aan betrokkenen. Andersom worden verwerkingen, waarvan een privacyverklaring wordt opgesteld, zoveel mogelijk (uniform) beschreven in het register.

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

Om de juistheid van persoonsgegevens van studenten ("studentgegevens") te borgen, worden continu updates vanuit het systeem Studielink doorgezet naar de grotere onderwijssystemen

[40] De RUG kijkt naar en sluit aan bij de mogelijkheden binnen de branche. Ook is organisatiebreed de wijze van communicatie met betrokkenen (over bijv. verzoeken tot rectificatie) vastgelegd en bewaakt.

binnen de RUG.[41] Hierbij wordt binnen Studielink onder meer gebruikgemaakt van DigID. De studentgegevens in Studielink worden op haar beurt weer gesynchroniseerd met de Basisregistratie Personen, DUO en IND.

Om de identiteit en persoonsgegevens van buitenlandse studenten te kunnen verifiëren worden (buitenlandse) paspoorten en ID-kaarten verwerkt. Tot op heden is dit een handmatig proces en is derhalve onderhevig aan een (menselijke) foutmarge.

Om buitenlandse paspoorten met grotere zekerheid te kunnen verifiëren op echtheid, werd in 2018 een project gestart binnen Studenten Informatie en Administratie ("SIA") om middels intelligente scanners de echtheid van identiteitsbewijzen te verifiëren. Middels deze scanners zijn meer accurate controles uit te voeren en levert de RUG een tijdsbesparing op. Het project is tot stilstand gekomen, omdat de technische realisatie binnen de RUG niet plaatsvindt.

Beleg de technische realisatie formeel binnen de RUG of laat de technische realisatie uitvoeren door een externe partij waarbij vanuit de RUG toezicht wordt gehouden.

Snel in Excel

Naast de (grote) onderwijssystemen worden binnen de RUG nog steeds studentgegevens verwerkt in Excel-bestanden en soortgelijke documenten.[42]

De studentgegevens binnen dergelijke documenten zijn per definitie niet actueel en in sommige gevallen incorrect.

De RUG dient de onderwijsprocessen in kaart te brengen waarvan de kwaliteit van de persoonsgegevens niet goed te borgen valt. Daarna dienen de verwerkingen met de hoogste risico's anders ingericht te worden. Om effectief en kostenefficiënt te werken heeft een instellingsbrede aanpak de voorkeur.

Correctie persoonsgegevens studenten

Een student die zijn naam, nationaliteit, verblijfplaats, huwelijkse staat en e-mailadres wil wijzigen kan terecht bij de Basisregistratie Personen ("BRP") van de overheid en in het systeem Studielink.

Persoonsgegevens van medewerkers

In 2019 is weinig tot niets gewijzigd ten aanzien van de kwaliteitsmanagement van de persoonsgegevens van medewerkers. Dit is begrijpelijk gezien de geplande transformatie van HR-processen en HR-systemen in januari 2020 in het kader van Best Practice 2020.

Wijziging en het actueel houden van persoonsgegevens van medewerkers ("medewerkersgegevens") vond plaats in de portal Do It

[41] Studielink synchroniseert met Progress.NET. Progress.NET heeft een aantal koppelingen met andere systemen.
[42] Een dergelijk beeld werd in 2018 reeds geschetst door eigenaren en beheerders van de systemen, maar ook in 2019 bevestigd door de decentrale studentenadministraties.

Yourself. Ook kon via de afdeling HR Services telefonisch of per e-mail een wijziging doorgevoerd worden.

Met de implementatie van AFAS[43] is een aantal systemen en koppelingen niet langer vereist. Dit komt in principe de kwaliteit en actualiteit van persoonsgegevens ten goede. Vanzelfsprekend is kwaliteitsmanagement van persoonsgegevens in één systeem beter te realiseren dan in meerdere systemen.

Binnen AFAS speelt zich een deel van de verwerking van medewerkersgegevens af. AFAS is gekoppeld aan Picobello welk systeem gegevens doorzet aan andere systemen, zoals Nestor. Tot hier is de borging van de kwaliteit goed te beheren.

De RUG kent ook een aantal “niet-gekoppelde” systemen zoals Ocasys (online onderwijscatalogus) en Syllabus Plus (opstellen roosters). Gegevens worden handmatig overgenomen van bijv. AFAS naar een dergelijk systeem, wat het beheer van de kwaliteit en actualiteit van persoonsgegevens te wensen over laat.

Binnen de RUG zijn niet alle systemen te koppelen met Picobello, omdat de processen binnen de verschillende faculteiten wisselend zijn vormgegeven. Kwaliteitsmanagement is echter niet (geheel) afhankelijk van technische koppelingen/maatregelen. Organisatorische borging is minstens net zo belangrijk, zo niet belangrijker.

De RUG dient te beschrijven hoe kwaliteitsmanagement er bij “niet-gekoppelde” systemen uit hoort te zien. Bewaken van de kwaliteit en actualiteit is daar onderdeel van.

Persoonsgegevens van onderzoekssubjecten

Het domein onderzoek wijkt duidelijk af van onderwijs en bedrijfsvoering. Dit komt omdat de individuele onderzoeker een zelfstandige verantwoordelijkheid heeft voor het beheer van de kwaliteit van de data (lees: persoonsgegevens). Het betreft een gedeelde verantwoordelijkheid waarbij de RUG als instelling verantwoord onderzoek dient te faciliteren.

Controle op de kwaliteitsmanagement binnen specifieke onderzoeksprojecten, anders dan op het verwerkingsniveau door de onderzoeker, vindt niet structureel en organisatiebreed plaats.[44]

In hoofdstuk 3 is reeds het wisselende kennisniveau van privacy en security bij onderzoekers aangestipt. Hetzelfde geldt voor de ethische commissies en de facultaire onderzoeksondersteuning. In principe kan dit leiden tot wisselend kwaliteitsmanagement van persoonsgegevens.

Het is derhalve niet per se de privacywetgeving die in dezen zorgt voor correcte en actuele persoonsgegevens. Onderzoekers binnen alle disciplines trachten namelijk de kwaliteit van

[43] Met AFAS wordt er gedoeld op AFAS Insite.
[44] Bewaking vindt incidenteel plaats door de ethische commissie, de facultaire onderzoeksondersteuning, het Research Data Office en/of de FG.

“hun” data optimaal te houden. Onderzoekers streven bij academisch onderzoek vanzelfsprekend naar kwaliteit en betrouwbaarheid van hun onderzoeksresultaten.

Op operationeel niveau wordt de borging hiervan binnen de RUG beschreven in het RDMP. De bescherming van persoonsgegevens is binnen het plan een onderdeel en wordt behandeld in de vorm van uitgangspunten als transparantie en verifieerbaarheid van onderzoek en hergebruik van onderzoeksgegevens.[45]

De afwegingen bij de daadwerkelijke bescherming van persoonsgegevens komen vaak pas aan bod bij de fase “toegang verschaffen tot data”.[46]

Daarbij spelen de FAIR-principes ook een rol. Deze worden behandeld in hoofdstuk 11.

Los van WMO-plichtig onderzoek (in samenwerking met het UMCG) kent de RUG geen specifieke richtlijnen ten behoeve van de kwaliteitsmanagement van persoonsgegevens in onderzoek. Wel wordt dit aspect behandeld in de Gedragscode WI en de Gedragscode voor gebruik persoonsgegevens in wetenschappelijk onderzoek[47] (“Gedragscode persoonsgegevens onderzoek”).

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.

Om de datakwaliteit binnen onderzoek met persoonsgegevens te borgen, is allereerst kennis bij de onderzoeker en de facultaire onderzoeksondersteuning vereist. Bij de RUG is onder meer educatief materiaal aanwezig in de vorm van de handleiding “Starting with a DPIA methodology for human subject research”.[48] Binnen de handleiding wordt het aspect datakwaliteit kort behandeld en toegelicht voor de onderzoeker.

De ethische commissies en de facultaire onderzoeksondersteuning dienen de onderzoeker te wijzen op voornoemde materiaal wanneer persoonsgegevens worden verwerkt binnen een onderzoek.

[45] M. van Berchum, & M.J. Grootveld, ‘Het beheren van onderzoeksdata’, *Handboek Informatiewetenschap*, IV B 475, Vakmedianet, 2016, p. 2-3.
[46] M. van Berchum, & M.J. Grootveld, ‘Het beheren van onderzoeksdata’, *Handboek Informatiewetenschap*, IV B 475, Vakmedianet, 2016, p. 16-17.
[47] De gedragscode stamt uit 2005 en is verouderd. Er wordt vanuit de VSNU gewerkt aan een nieuwe gedragscode.
[48] Ook de e-learningmodule Privacy in research: “asking the right questions” is hiervoor geschikt.

8. Bewaren van persoonsgegevens

De wet- en regelgeving kent veel bewaartermijnen. Desondanks zijn veel bewaartermijnen niet formeel vastgesteld. De AVG bevat voor de verwerking van persoonsgegevens geen bewaartermijnen, maar wel het beginsel "opslagbeperking". Dit houdt in dat persoonsgegevens niet langer worden bewaard, dan noodzakelijk voor de doelen waarvoor deze zijn verzameld.

Binnen de RUG zijn veel bewaartermijnen niet vastgesteld of worden deze niet nageleefd. Om bewaartermijnen te kunnen bepalen, is het noodzakelijk om de specifieke doelen van verwerkingen helder te hebben. Het vaststellen van doelen en als verantwoordelijke (lees: de RUG) daaraan houden is daarom een ander beginsel: "doelbinding."[49]

Een handreiking voor bewaartermijnen is echter wel te vinden in de zogenaamde Selectielijst voor universiteiten en UMC's ("Selectielijst").[50] De Selectielijst biedt met name handvatten voor bewaartermijnen in onderwijs(processen) en bedrijfsvoering.

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.

E-mail kent geen bewaartermijnen

Los van de bewaartermijnen specifiek voor één van de drie domeinen, maken middelen zoals e-mail het voor de RUG lastig. Binnen het medium e-mail is het kunnen voldoen aan de plicht om te verwijderen tot op heden grote uitdaging. Er zijn meerdere trotse medewerkers met reeds één of meer jubilea achter de rug, maar die nog wel de e-mail van de eerste werkdag in de e-mailbox hebben staan.

De e-mail is in veel gevallen het collectief archief van de RUG en daarmee verwerkt zij van (tien)duizenden mensen persoonsgegevens. In veel gevallen worden

[49] Meer over doelbinding in hoofdstuk 5.
[50] De Selectielijst Universiteiten en Universitair Medische Centra 2020 is vastgesteld op 31 januari 2020.

persoonsgegevens langer verwerkt dan noodzakelijk. Daarmee voldoet de RUG niet aan de opslagbeperking(, doelbinding en dataminimalisatie).[51]

Naast de e-mail is de omgang met bewaartermijnen binnen de drie grote categorieën van betrokkenen (studenten, medewerkers en onderzoekssubjecten) verschillend ingericht. Hieronder wordt per domein de omgang beschreven.

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 beargumenteerd 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.[52]

Persoonsgegevens medewerkers

Met de komst van AFAS wordt de mogelijk geboden om persoonsgegevens van personeel te verwijderen bij het bereiken van het einde van een bewaartermijn. Protocollen en organisatiebrede inbedding van bewaartermijnen binnen het dossier van de medewerker zijn nog niet formeel vastgesteld.

Het vele maatwerk in de dienstverbanden bij de RUG, maakt het (geheel) geautomatiseerd verwijderen van persoonsgegevens vooralsnog geen veilige optie. Zonder handmatige controle binnen AFAS bestaat de kans op het per ongeluk verwijderen van persoonsgegevens.

Het opstellen van de zogenaamde 'best practices' en het duidelijk formuleren van verantwoordelijkheden is daarbij essentieel wil de RUG de bewaartermijnen goed naleven. Integratie van het archief binnen AFAS biedt hierbij de nodige houvast.

Persoonsgegevens onderzoekssubjecten

Binnen het onderzoeksveld worden de bewaartermijnen in beginsel overgelaten aan de disciplines. De Selectielijst Universiteiten en Universitair Medische Centra 2020[53] beschrijft dit als volgt: "[..] *Daarbij moet dan rekening worden gehouden met de aard van de data, de waarde van de data, persoonsgegevens en manier van opslag. Ook dient de herbruikbaarheid (dus de*

[51] Hetzelfde risico geldt voor persoonsgegevens binnen de Business Intelligence Portal.
[52] Meer over de gestandaardiseerde processen in Hoofdstuk 5 Doelbinding en intern toezicht.
[53] In 2019 werd er voor beleidstukken al met een conceptversie van de Selectielijst gewerkt.

waarde) van de data te worden getoetst aan de belangen voor maatschappelijke bewaring zoals 'open science'. [..]"

Gemiddeld genomen wordt 10 jaar aangehouden bij niet-medisch onderzoek en 15 jaar bij medisch onderzoek.

Ondanks de discipline-specifieke bewaartermijnen gelden er vanuit de AVG afwijkende regels omtrent bewaartermijnen binnen het domein onderzoek. Zo is 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.

De RUG kent geen sectorspecifiek of instellingsbreed beleid omtrent de bewaartermijnen van persoonsgegevens in onderzoek. Onderzoekers zijn derhalve aangewezen op de eigen interpretatie van de gedragscodes[54] en de privacywetgeving.

Voor het bepalen van bewaartermijnen is het belangrijk om per sector/onderzoeksgebied te kijken naar de doelen voor langdurige opslag van persoonsgegevens. Twee belangrijke doelen zijn: 1) voor hergebruik in (nieuw) onderzoek en; 2) voor replicatie en verificatie van het onderzoek.

Binnen de RUG kan gestart worden met het opstellen van kaders die per faculteit (of onderzoeksgebied) ingevuld dienen te worden. Zo kunnen sectorspecifieke richtlijnen vorm krijgen. Bij het opstellen van richtlijnen is de inbreng van onderzoekers cruciaal.

[54] 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

Zonder security geen privacy. Een goede borging van de privacy vraagt om passende technische en organisatorische maatregelen. De RUG neemt ten behoeve van de verwerking van persoonsgegevens beveiligingsmaatregelen die preventief, repressief en correctief van aard zijn. Het vereiste niveau aan beveiliging is afhankelijk van de kwantiteit en kwaliteit van de persoonsgegevens. Hoe gaat de RUG in tijden van ransomware en soortgelijke uitdagingen om met de beveiliging?

De AVG schrijft geen specifieke (technische) beveiligingsmaatregelen voor. De wet vraagt aan de verantwoordelijke (lees: de RUG) om maatregelen te nemen die passen bij de stand van de techniek, uitvoeringskosten, omvang en context van de verwerkingen en hun doelen.

Met name in het laatste kwartaal van 2019 is de RUG in haar volwassenheid gegroeid. Zo vinden er binnen de RUG beveiligingsrisicoanalyses plaats en worden maatregelen beschreven en uitgevoerd. Ook heeft de RUG een organisatiebreed informatiebeveiligingsplan vastgesteld waarbij de bescherming van persoonsgegevens is meegenomen.

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.

Om een beeld te krijgen van de externe (digitale) dreigingen en daarmee de risico's, is gekeken naar de dreigingsbeelden van de NCSC en SURF.[55] Enkele concrete risico's komen verderop in dit hoofdstuk aan bod onder "Buitenlandse actoren".

Gezien de dreigingsbeelden en de snelheid waarmee (nieuwe) risico's zich ontwikkelen, is het voor de RUG belangrijk om toe te werken naar periodieke risicoanalyses. Daarbij dient het nemen van mitigerende maatregelen plaats te vinden volgens een RUG-brede en formeel vastgestelde wijze.

Het neerleggen van beslissingsbevoegdheid omtrent het minimale beveiligingsniveau op

[55] Het dreigingsbeeld van de NCSC: https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/juni/12/cybersecuritybeeld-nederland-2019/CSBN2019.pdf en SURF: https://www.surf.nl/files/2020-02/surf-cyberdreigingsbeeld-2019-2020.pdf.

decentraal niveau is niet wenselijk. Zoals we ook bij de Universiteit in Maastricht zagen, is één computer met gebrekkige beveiliging voldoende voor cybercriminelen om een succesvolle aanval uit te voeren op de overige universitaire systemen.

Het niveau van de basisbeveiliging[56] dient derhalve centraal te worden gedefinieerd en te worden bewaakt.

Governance bij informatiebeveiliging en informatiemanagement

Los van de basisbeveiliging en het informatiebeveiligingsplan dient de RUG te kijken naar de governance rond de beveiliging van persoonsgegevens. Momenteel is de inrichting en borging van de beveiliging deels formeel[57] en deels informeel geregeld. Meer specifiek: het beveiligen is geen structureel onderdeel van het ontwerp en de opzet van (nieuwe) verwerkingen van persoonsgegevens.

De taken, verantwoordelijkheden en bevoegdheden bij de beveiliging van persoonsgegevens dienen op organisatiebrede wijze te worden gedefinieerd en vast te worden gesteld. Daarnaast is de implementatie en bewaking van die taken, verantwoordelijkheden en bevoegdheden onmisbaar.

Naast voornoemde risico is er een andere reden om te kijken naar de organisatorische inrichting bij de RUG. Kennis en kunde van informatiebeveiliging is geconcentreerd bij het CIT. CIT is de interne IT-leverancier van de RUG.[58] Beveiliging van informatie(technologie) is niet haar primaire taak. Desondanks zijn de twee security managers die de RUG rijk is, geplaatst bij het CIT en leggen verantwoording af aan de directie van het CIT.

Volledig onafhankelijk kunnen de security managers derhalve hun werk niet uitvoeren. Daarbij komt dat het niveau van de beveiliging mede afhankelijk is van de middelen en prioriteiten van het CIT. De afweging wordt niet per definitie gemaakt vanuit het perspectief van de gehele organisatie of in het licht van passende beveiliging van persoonsgegevens.[59]

De RUG dient zorg te dragen voor een passende positionering van de informatiebeveiligingsorganisatie, om beleid, middelen en prioriteiten optimaal te beleggen.

---

[56] Binnen de RUG is de basisbeveiliging vastgelegd in de RUG Baseline.
[57] Het Informatiebeveiligingsbeleid van de RUG beschrijft de governance rondom de informatiebeveiliging. Deze wordt in de “Regulation annual information security and data protection plan” in detail uitgewerkt.
[58] Zie art. 8.2.1 van het Bestuurs- en beheersreglement van de Rijksuniversiteit Groningen: [..] in het [..] Centrum voor Informatietechnologie wordt computer- en nevenapparatuur voor de automatische verwerking van gegevens beheerd en, onder door het College van Bestuur, de directeur gehoord, te stellen voorwaarden, ter beschikking gesteld ten behoeve van het wetenschappelijk onderwijs en onderzoek, het bestuur en het beheer van de universiteit.
[59] Deze afweging is relevant voor veel van de trajecten om risico’s, benoemd in dit hoofdstuk, weg te nemen.

Naast de governance achter de informatiebeveiliging, kent de RUG een aantal relevante onderwerpen die variëren van intern gebruik van persoonsgegevens tot gebrekkige beveiliging bij verwerkers. De meest relevante en urgente onderwerpen worden hierna beschreven.

Verwerking persoonsgegevens binnen de bedrijfsvoering

De bedrijfsvoering is verweven met de alledaagse verwerkingen binnen de RUG. Op de werkvloer is winst te behalen met betrekking tot beveiliging. Hieronder worden enkele risico's benoemd en oplossingen voorgesteld.

Onbeveiligde verwerking van (bijzondere) persoonsgegevens

E-mail is naast de Y-schijf en Google Drive nog steeds dé manier om documenten met (bijzondere) persoonsgegevens van A naar B te krijgen. Binnen de RUG worden de meeste e-mails niet versleuteld. Dit betekent dat kwaadwillenden die e-mail onderscheppen, deze ook kunnen lezen (en aanpassen).

Na 2018 is de e-mail niet beter beveiligd of versleuteld. Dit geldt voor de e-mailcommunicatie binnen een dienst/faculteit, maar ook tussen faculteiten en diensten. Illustratief is de verzending van identiteitsbewijzen van studenten aan de afdeling SIA.

Voor het interne e-mailverkeer is de encryptie die Google Suite for Education aanbiedt een eerste stap. Deze encryptie is op dit moment beschikbaar. Daarnaast zal de RUG moeten kijken naar alternatieven voor e-mail, zoals Unishare.

Bij het aanbieden van veiligere alternatieven dient gebruiksvriendelijkheid een grote rol te spelen. Gebruiksgemak en richtlijnen rondom de veilige verzending van (bijzondere) persoonsgegeven zijn bepalend voor een succesvolle overstap.

Naast de reguliere @rug.nl-e-mailadresssen maken veel medewerkers van de RUG gebruik van hun persoonlijke e-mailadres (@gmail.com, @live.com, @hotmail.com) om met collega's, studenten en onderzoekssubjecten te e-mailen. De leveranciers van deze (meestal gratis) e-mailaccounts doorzoeken de e-mail, koppelen vervolgens de geïndexeerde gegevens aan andere bronnen om uitgebreide gebruikersprofielen te kunnen creëren. Deze profielen worden gebruikt voor verschillende doelen, zoals marketing.

Wijs medewerkers op het oneigenlijk gebruik van persoonlijke e-mailaccounts binnen bedrijfsvoering, onderwijs en onderzoek. Communicatie hierover via de centrale kanalen is zeer wenselijk. Bied eventueel een alternatief aan indien het eigen @rug.nl-e-mailadres niet voldoet voor de specifieke doelen.

BYOD

Bij de RUG wordt door de medewerkers veel gebruikgemaakt van persoonlijke apparaten onder de noemer "Bring you own device" (BYOD). BYOD vergroot de flexibiliteit en het

gebruiksgemak. Deze vloot aan onbeheerde apparaten vormt voor de RUG echter wel een risico. (Persoons)gegevens blijven niet binnen beheerde IT-infrastructuur van de RUG.

Verloren en gestolen laptops, tablets en telefoons leveren de RUG jaarlijks enkele datalekken op.[60]

In tijden van een crisis zoals de coronacrisis, wordt het meeste werk uitgevoerd op apparaten die niet door de RUG worden beheerd.

Bij de RUG is toezicht op het niveau van beveiliging van BYOD vrijwel afwezig. Onvoldoende maatregelen, zoals encryptie van harde schrijven, leiden tot zwaardere categorieën datalekken wanneer BYOD kwijtraken of gestolen worden.

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

In het verlengde van BYOD, liggen de uitgegeven apparaten. De RUG vertrouwt laptops en tablets toe aan haar medewerkers. In veel gevallen worden de uitgeleende apparaten niet geregistreerd. Het is derhalve voor de RUG momenteel niet mogelijk om de Baseline effectief te borgen op dit onderwerp. De Baseline vraagt om het formatteren en/of vernietigen van het apparaat na het einde van het dienstverband van de medewerker –of- bij de buitengebruikstelling van het apparaat zelf.

Het Facilitair Bedrijf kan technisch en organisatorisch de ter beschikking gestelde apparaten registreren. Zij wordt echter niet (altijd) geïnformeerd door de intern verantwoordelijken over uitgiftes. Dit dient een vast stap te zijn binnen het proces van uitgifte.
Ook zal controle op deze apparaten onderdeel uit moeten maken van het exit-protocol bij de RUG om de beveiliging van persoonsgegevens correct te kunnen borgen.

Een nauwkeurigere registratie van apparaten kan daarnaast een bijdrage leveren in het beperken van fraude en/of verduistering.

Versleuteling uitgegeven apparaten

Naast de registratie van uitgegeven apparaten is de beveiliging op diezelfde apparaten een belangrijk punt. Diefstal en verlies van apparatuur is onoverkomelijk, het kwijtraken van data en inbreuk op de bescherming van persoonsgegevens niet.

[60] Verlies of diefstal van apparatuur wordt niet altijd gemeld. Het aantal datalekken ligt om die reden hoger dan het vermelde aantal in hoofdstuk 12 Datalekken.

Reeds in 2018 is binnen de RUG het Project versleutelen gegevensdragers opgestart. Middels het project zouden de werkprocessen en de infrastructuur worden opgeleverd om universiteitsbreed desktop pc's en laptops te versleutelen. De verwachte oplevering van de infrastructuur was: Q2 2019. Het project is halverwege 2019 "on hold" gezet en heeft daarna geen gevolg meer gekregen.

Stel een realistische planning op en rond het Project versleutelen gegevensdragers af. Voor een effectieve toepassing binnen de gehele RUG is organisatorische inbedding van belang. Het advies is derhalve om HR en het Facilitair Bedrijf hierbij te betrekken.

Het voornoemde project behelst enkel de desktop pc's en laptops. Versleuteling van tablets en andere mobiele apparatuur die persoonsgegevens verwerken dient veelal door de medewerker zelf gerealiseerd te worden. Zonder awareness en ondersteuning vanuit RUG, leveren deze onversleutelde apparaten nog steeds een hoog risico op voor de bescherming van persoonsgegevens.

Ontwikkelen in een OTAP-omgeving

Het laatste punt van aandacht binnen het domein bedrijfsvoering ziet op de ontwikkeling van applicaties en diensten. Binnen de RUG worden nog steeds veel applicaties, diensten en producten ontwikkeld.

Bij die ontwikkeling worden nog te vaak (bijzondere) persoonsgegevens gehanteerd om te testen zonder dat daar een noodzaak voor is aan te wijzen. Naar aanleiding van het gebruik van live data in de testomgevingen heeft de RUG reeds enkele datalekken[61] veroorzaakt.

Draag zorg voor een goed ingerichte OTAP-omgeving (Ontwikkel, Test, Acceptatie, Productie) waarbij bij de ontwikkel- en testfase géén persoonsgegevens worden gehanteerd. Het besluit over een uitzondering op deze regel zou daarbij niet enkel bij de ontwikkelaar(s) mogen liggen. Een functiescheiding is derhalve nodig.

Beveiliging Progress.NET (vervolg)

In de *Jaarrapportage bescherming persoonsgegevens RUG 2018* ("Jaarrapport 2018") is de applicatie Progress.NET uitvoerig aan bod gekomen. In de applicatie bevinden zich van tienduizenden studenten en alumni de persoonsgegevens. Daarnaast worden er veel gevoelige en bijzondere persoonsgegevens verwerkt.[62] De (gebrekkige) inrichting van de applicatie was in het verleden oorzaak van enkele incidenten.

Afgelopen jaar heeft de RUG in samenwerking met de ontwikkelaar (UOCG Market BV) enkele stappen gezet

[61] In het merendeel van de gevallen was er sprake van een datalek met een laag risicoprofiel.
[62] Naast naam, adres, tentamencijfers en judicia worden bijvoorbeeld ook notities van studieadviseurs en zelfs psychologen beheerd in Progress.NET

om de risico's voor de betrokkenen (studenten en alumni) te beperken. De twee belangrijkste stappen:

1. het aantal ontwikkelaars dat toegang heeft tot zeer gevoelige en bijzondere persoonsgegevens is sterk teruggebracht. Ook zijn er extra technische drempels opgeworpen in de database om te voorkomen dat ontwikkelaars per ongeluk toch inzage hebben in persoonsgegevens;
2. de ontwikkelaar heeft het testen met live data in de ontwikkelomgeving beëindigd.

Ondanks de stappen voorwaarts zijn er binnen Progress.NET nog veel (gevoelige en bijzondere) persoonsgegevens toegankelijk voor medewerkers waarvoor dit niet noodzakelijk is. De oorzaak hiervan ligt grotendeels in de complexiteit van het doorvoeren van uniforme gebruikersprofielen binnen het systeem terwijl faculteiten verschillende werkwijzen en rollen hanteren.

De beginselen dataminimalisatie en vertrouwelijkheid moeten navolging krijgen in Progress.NET. Dit betekent concreet dat rollen en rechten fijnmaziger ingericht moeten worden én periodieke controle op de rechten van de gebruikers moet plaatsvinden.

Buitenlandse actoren

Vorig jaar werd in de jaarrapportage van de FG aandacht besteed aan de risico's van de Amerikaanse CLOUD Act.[63] De risico's blijven bestaan, maar zijn niet langer de enige aandachtspunten.

Het is al langer bekend dat ook andere landen uit zijn op kennis die zich in Nederland bevindt. Universiteiten met veel specialistische kennis zijn aantrekkelijk. De NCSC beschrijft in haar dreigingsbeeld het volgende: "landen als China, Iran en Rusland hebben offensieve cyberprogramma's gericht tegen Nederland."

De NCSC ziet daarbij digitaal onveilige producten en diensten als de achilleshiel binnen organisaties. Deze vormen een fundamentele oorzaak van incidenten.

Ook binnen de RUG zijn digitaal onveilige producten en diensten aanwezig. Hierbij kan gedacht worden aan systemen die "end-of-life"[64] zijn, maar ook applicaties van eigen makelij die niet voldoen aan de beveiligingsstandaard die bijv. de RUG baseline biedt.

Het beveiligingsplan 2020/2021 van de RUG voorziet in veel effectieve maatregelen, maar wordt niet periodiek opgesteld. Om externe risico's zo veel mogelijk te kunnen beperken zal het beveiligingsplan onderdeel moeten uitmaken van een PDCA-cyclus.

[63] Deze Act verplicht Amerikaanse bedrijven om op verzoek van de Amerikaanse autoriteiten data die buiten de VS op servers zijn geplaatst aan te leveren. Verwerkers van de RUG, zoals Google en Microsoft vallen hieronder.
[64] Dit betekent dat hardware of software niet langer ondersteund wordt door een leverancier of organisatie. Updates om de beveiliging te verbeteren worden niet meer ontwikkeld en/of aangeboden.

Beveiliging bij onderzoek met persoonsgegevens

In hoofdstuk 6 Register is reeds beschreven dat onderzoeken met persoonsgegevens beperkt in kaart zijn gebracht. Indien dergelijke onderzoeken niet “geregistreerd” zijn, is inhoudelijke beoordeling van de beveiliging praktisch onmogelijk.

Los van het gebrek aan overzicht is het niveau van beveiliging bij onderzoek veelal informeel en op verwerkingsniveau bepaald. Dit betekent dat het niveau in beginsel afhankelijk is van de (hoofd)onderzoeker, de onderzoeksondersteuning en/of de onderzoeksregels binnen de faculteit.

Onderzoekers dienen voorafgaand aan het onderzoek geïnformeerd te worden over passende technische en organisatorische maatregelen. Meer specifiek moet een onderzoeker begrijpen welke maatregelen relevant zijn voor zijn/haar type onderzoek.

Momenteel bieden het CIT en RDO technische en organisatorische ondersteuning aan onderzoekers om onderzoeksdata (veiliger) te kunnen verwerken. De beschikbare middelen en ondersteuning worden getoond op de website van Data Federation Hub. De website fungeert als overzicht en “menukaart” van diensten, maar adviseert niet over het gebruik van specifieke maatregelen bij specifieke vormen van onderzoek.

Building blocks in onderzoek

Om te komen tot de juiste maatregelen binnen een (nieuw) onderzoek is het doen van een DPIA in beginsel het uitgangspunt.[65] Een dergelijke risico-inventarisatie vergt echter tijd, kennis en een team van professionals. Aangezien er binnen de RUG elk jaar al meer dan 1000 onderzoeken met persoonsgegevens plaatsvinden lijkt het uitvoeren van 1000+ DPIA’s niet erg (kosten)efficiënt. Daarnaast is er veel overlap in de omgang met persoonsgegevens binnen de verschillende onderzoeken.

Faculteiten dienen onderzoeksscenario’s te beschrijven waaraan zogenaamde sets van maatregelen (“building blocks”) worden gekoppeld.

De RUG kent al een reeks aan belangrijke building blocks, waaronder:

- Pseudonimiseringsdienst[66]
- Anonimiseringsdienst[67]
- Data koppelen
- Database versleuteling
- Virtual Reseach Workspace

[65] Het richtsnoer “Starting with a DPIA methodology for human subject research” helpt de onderzoeker bij vragen over het DPIA.
[66] Bij pseudonimiseren blijft de bruikbaarheid van de data hoog, terwijl de risico’s voor betrokkenen sterk worden verminderd.
[67] Geanonimiseerde gegevens worden onder de AVG niet langer gezien als persoonsgegevens. De verwerking van anonieme gegevens valt derhalve niet langer onder de AVG.

10. Informatieverstrekking en rechten betrokkenen

De RUG verwerkt persoonsgegevens van studenten, medewerkers en onderzoekssubjecten ("betrokkenen"). Daarbij is transparant handelen een voorwaarde: de betrokkene moet in beginsel geïnformeerd worden over de verwerking. De betrokkene heeft op zijn 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.[68]

De RUG kent een algemene privacyverklaring. Deze omschrijft de verwerkingen van persoonsgegevens binnen de RUG op een hoog abstractieniveau. Het informeren van betrokkenen op een dergelijk abstractieniveau is niet voldoende om te spreken van transparantie conform de AVG.

Daarom is de RUG in een hoog tempo verklaringen aan het opstellen voor de betrokkenen binnen alle domeinen. Hierbij worden verwerkingen met het hoogste risico als eerste beschreven. Ook hanteert de RUG een standaard template en een nieuwe compacte versie van de privacyverklaring.[69] De compacte versie verhoogt de leesbaarheid en verduidelijkt de verwerking met visuele elementen.

Voornoemde standaarddocumenten voor het informeren van betrokkenen worden nog niet binnen alle faculteiten en diensten gehanteerd wanneer zij persoonsgegevens verwerken.

De RUG dient de toepassing van de standaarddocumenten te stimuleren en te bewaken binnen de faculteiten en diensten.

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.

[68] De belangrijkste rechten zijn opgenomen in artt. 15 – 22 AVG.
[69] Een voorbeeld is bijgevoegd als Bijlage 2. Compact model privacyverklaring RUG

Centraal Loket Privacy

Om tegemoet te komen aan alle verzoeken van de betrokkenen, hanteert de RUG het Centraal Loket Privacy ("Loket"). Betrokkenen kunnen hier een inzageverzoek of wijzigingsverzoek indienen. In samenwerking met de privacy- en securitycoördinatoren wordt vanuit het Loket een antwoord geformuleerd en/of acties uitgezet.

Niet alle verwerkingen binnen de RUG zijn in kaart gebracht, dan wel verlopen anders dan in het register beschreven. Dit maakt het beantwoorden van verzoeken van betrokkenen zeer arbeidsintensief en is het tijdig[70] beantwoorden een uitdaging.

Aantallen inzageverzoeken en overige verzoeken

In 2019 heeft de RUG de volgende verzoeken op grond van de AVG ontvangen:

Recht op inzage:	**3**
Recht op rectificatie:	**0**
Recht op verwijdering[71],[72]:	**34**
Recht op dataportabiliteit:	**0**

Van deze verzoeken heeft de RUG **3** inzageverzoeken en **10** verzoeken tot verwijdering 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

Binnen het domein onderzoek gelden afwijkende regelen ten aanzien van de verwerking van persoonsgegevens. Er kan namelijk worden afgeweken van een aantal rechten van onderzoekssubjecten.[73] Dit kan betekenen dat de RUG besluit om het onderzoekssubject geen inzage te geven in zijn/haar gegevens. Ook kan afgeweken worden van het recht op verwijdering indien daardoor het onderzoek onmogelijk wordt of ernstig in gedrang dreigt te worden gebracht.[74]

De bovenstaande uitzonderingen en de handelwijze in het geval van (overige) verzoeken van onderzoekssubjecten zijn binnen de RUG voor veel onderzoekers en onderzoeksondersteuners niet bekend. Het vergoten van kennis bij deze twee groepen zal derhalve gewenst zijn, zoals in hoofdstuk 3 is beschreven.

---

[70] De RUG heeft in principe één maand om te reageren op het verzoek van de betrokkene. Bij een (algemeen) inzageverzoek betekent dat het overleggen van alle verwerkingen met de persoonsgegevens van die betrokkene.
[71] In 24 van de 34 gevallen ging het om een geautomatiseerd verzoek tot verwijdering ("Data Removal Request").
[72] Niet elk verzoek om verwijdering hoeft gehonoreerd te worden. De AVG 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.
[73] Regels binnen het wetenschappelijk onderzoek zijn terug te vinden in art. 89 lid 2 AVG jo. art. 44 UAVG.
[74] Deze beperking van het recht op verwijdering wordt gevonden in art. 17 lid 3 sub d AVG.

11. Verwerkersovereenkomsten en doorgifte

De RUG zet honderden organisaties in die in opdracht van haar persoonsgegevens verwerken. Deze verwerkers worden verzocht een passende bescherming te hanteren bij die verwerkingen. De passende beschermingsmaatregelen vormen de kern van een verwerkersovereenkomst.[75] Eenzelfde set aan passende beschermingsmaatregelen is ook vereist indien persoonsgegevens buiten de EER[76] worden verwerkt.

Het doorzetten van persoonsgegevens aan derden wordt “doorgifte” genoemd. Veel doorgiftes vinden plaats naar verwerkers van de RUG. Denk aan AFAS (*Shared Services*), UOCG Market BV (*Progress*) en Blackboard Inc. (*Nestor*). Ook binnen onderzoek vindt (on)bewust doorgifte plaats van persoonsgegevens onder meer in het kader van “open science”.

Bij het inzetten van verwerkers begint de borging van een zorgvuldige omgang met persoonsgegevens met het maken van afspraken. Deze afspraken worden vastgelegd in een verwerkersovereenkomst. De RUG hanteert hierbij een standaard-verwerkersovereenkomst, gestoeld op het landelijke model van SURF.[77]

Controleren of afspraken worden nageleefd is stap twee. De RUG kan met de verwerker overeenkomen dat de controle op de passende bescherming(smaatregelen) door een derde partij (auditor) wordt uitgevoerd of door de RUG zelf. Stap twee wordt door de RUG sporadisch gezet.

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.

[75] De verplichting om een verwerkersovereenkomst te sluiten met verwerkers wordt gevonden in art. 28 lid 3 AVG.
[76] Europese Economische Ruimte bestaat uit de EU-landen met daarbij Liechtenstein, Noorwegen en IJsland.
[77] SURF is een coöperatie van universiteiten, hogescholen en mbo-instellingen die werken aan ICT-innovatie.

Beheer verwerkersovereenkomsten

In 2019 heeft de RUG een enorme slag gemaakt voor wat betreft het afsluiten van verwerkersovereenkomsten. Op dit moment heeft de RUG met circa honderd verwerkers een getekende verwerkersovereenkomst.

Van de verwerkersovereenkomsten die op centraal niveau bekend zijn is een overzicht met de statussen aanwezig. De route om verwerkersovereenkomsten af te sluiten is beter bekend geworden bij de decentrale eenheden. De P&S-coördinatoren weten de privacysectie van ABJZ te vinden. ABJZ is niet de enige dienst die grote aantallen overeenkomsten verwerkt. Ook diensten/faculteiten verwerken grote aantallen en voelen zich bij tijden genoodzaakt om extra (juridisch) personeel in dienst te nemen.[78]

Verder wordt er RUG-breed gewerkt met een standaardverwerkersovereenkomst. Enkel in uitzonderlijke situaties wordt hiervan afgeweken. Op deze manier worden de eisen die de RUG aan derden stelt geüniformeerd en zijn deze voor eenieder helder.

Contracteren met verwerkers gebeurt binnen de RUG op centraal en decentraal niveau. Decentraal is men niet altijd bekend met de (standaard)verwerkersovereenkomst.[79] De doorgifte van persoonsgegevens kent derhalve niet altijd de eisen die centraal zijn vastgelegd. Ook kan het passende beveiligingsniveau op centraal niveau niet bewaakt worden. Een RUG-brede beheeromgeving voor (verwerkers)overeenkomsten is afwezig, dan wel niet in gebruik.

(Verwerkers)overeenkomsten dienen een beheerde en gestructureerde plek te krijgen. De RUG kan enkel op die wijze borgen dat zij inzicht heeft in alle verwerkers en de gestelde eisen omtrent de bescherming van persoonsgegevens.

Naleving door verwerkers

De RUG komt met haar verwerkers overeen om specifieke beveiligingsmaatregelen te treffen. Als verantwoordelijke is de RUG verplicht om de naleving daarvan te (laten) controleren.

Audits ten aanzien van de bescherming van de persoonsgegevens worden door de RUG zelden tot nooit uitgevoerd. Het besluit tot auditen gebeurt momenteel informeel en is afhankelijk van de keuze van een (decentrale) afdeling. Deze handelwijze komt overeen met die in het jaarrapport 2018.

Bepaal aan de hand van het risico van een verwerking of en wanneer een audit wordt uitgevoerd door een derde partij of de RUG bij een verwerker.

Naar aanleiding van een datalek binnen het domein onderzoek is de RUG daadwerkelijk overgegaan tot het laten uitvoeren van een audit. Vanaf het daadwerkelijke incident tot de

[78] Een voorbeeld is de afdeling ESI binnen het CIT. ESI heeft te maken met een groot aantal applicaties waarvoor afspraken met leveranciers vereist zijn.
[79] Denk hierbij aan de docent die online applicaties inzet en zelf de overeenkomst met de leverancier tekent.

uiteindelijke audit besloeg meer dan 12 maanden.[80] Gedurende deze tijd lag het desbetreffende onderzoek stil. De uiteindelijke resultaten van een audit zijn na een dergelijke lange termijn niet meer actueel en beperkt bruikbaar, omdat er naar de situatie gekeken wordt ten tijde van het incident.

De lange doorlooptijd vanaf een incident tot de daadwerkelijke controle op de technische en/of organisatorische maatregelen moedigt de onderzoeker niet aan om een incident te melden.

De RUG dient helder te beschrijven hoe zij omgaat met een verwerking/een verwerker na afloop van een incident waarbij de verwerker (mogelijk) onvoldoende maatregelen zou hebben genomen. Tevens dienen ABJZ en overige betrokken afdelingen afspraken te maken om een vlotte uitvoering van een audit te bewerkstelligen.

Doorgifte van onderzoeksgegevens

Binnen onderzoek is tegenwoordig het devies “open science”. Daarbij worden veelal de FAIR-principes gehanteerd. Bij hergebruik van onderzoeksdata is het uitgangspunt “open, tenzij.” Om die reden zouden datasets zoveel mogelijk gepseudonimiseerd moeten worden, zodat datasubjecten in principe niet terug te herleiden zijn.

Het pseudonimiseren vindt binnen de RUG niet altijd (correct) plaats. Zo zijn sets met data met daarin e-mailadres, telefoonnummer en/of adres terug te vinden in de zogeheten “data repositories”, zoals DataverseNL.

Inzet op heldere communicatie over de bestaande pseudonimiseringsdiensten, zoals in hoofdstuk 9 is vermeld, is belangrijk. Kennis hierover dient ook bij de ethische commissies en de facultaire onderzoeksondersteuning te liggen.

Doorgifte buiten de EER en Brexit

Veel persoonsgegevens worden verwerkt buiten de grenzen van de EER (de EU inclusief Noorwegen, Liechtenstein en IJsland). Dit gebeurt voor onderzoek, maar ook voor applicaties binnen de domeinen onderwijs en bedrijfsvoering. Hierbij kan gedacht worden aan Nestor (Blackboard) waarbij een deel van de persoonsgegevens in de Verenigde Staten wordt verwerkt.

Het niveau van bescherming van persoonsgegevens die binnen de EER gehanteerd wordt is hoog. Hetzelfde niveau wordt in veel andere werelddelen niet gehaald. Toch is doorgifte naar die werelddelen toegestaan indien aan een van de voorwaarden uit de AVG wordt voldaan.

[80] De (technische) audit nam zelf twee dagen in beslag.

Hierbij kan gedacht worden aan zogenaamde adequaatheidsbesluiten[81], standaard- of ad-hocbepalingen voor gegevensbescherming[82] en gedragscodes.

De RUG dient heldere richtlijnen op te stellen waaruit blijkt hoe om te gaan met de doorgifte van persoonsgegevens en onder welke voorwaarden er al dan niet doorgifte plaatsvindt naar specifieke landen/werelddelen.

Op 31 januari 2020 heeft het Verenigd Koninkrijk de Europese Unie verlaten. Tot 1 januari 2021 geldt een overgangsfase waarbij de EU-regelgeving (zoals de AVG) van kracht blijft. Daarna is de omgang met het Verenigd Koninkrijk afhankelijk van de gemaakte afspraken. Een adequaatheids-besluit valt te verwachten.

Bij een no-dealbrexit wordt het Verenigd Koninkrijk een zogenaamd derde land en gelden de bovengenoemde voorwaarden uit de AVG. De (privacy)juristen binnen de RUG zijn bekend met deze voorwaarden en hanteren deze reeds voor andere derde landen.

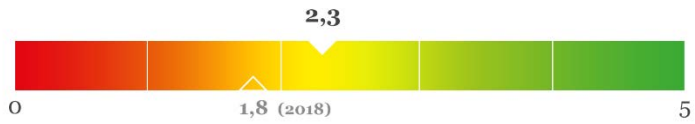
[81] Dit is een besluit van de Europese Commissie waarin is vastgesteld dat specifiek land een “passend beschermingsniveau waarborgt”.
[82] Standaardcontracten met een aantal minimale vereisten welke zijn goedgekeurd door de Europese Commissie.

12. Datalekken

In 2019 was het aantal datalekken vergelijkbaar met dat van 2018. Binnen de organisatie is het begrip van het fenomeen nog beperkt. Zo zien de meeste datalekken niet op het verlies van USB-sticks, maar op de onrechtmatige verwerking van persoonsgegevens in systemen en e-mail. Met de komst van nieuwe leden in het CvB is ook de borging van maatregelen na afloop van een datalek verbeterd.

In de privacywetgeving wordt niet gerept over “datalekken”, maar over “inbreuk in verband met persoonsgegevens.” Voor de leesbaarheid van deze rapportage wordt “datalekken” gehanteerd. Om de meldingsbereidheid te vergroten zou “inbreuk in verband met persoonsgegevens” mogelijk verstandiger zijn. Medewerkers en studenten hebben namelijk een sterk ingekleurd en te beperkt beeld van een datalek.[83] *De verloren USB-stick* is namelijk hét standaardvoorbeeld, maar is niet illustratief voor het gemiddelde datalek bij de RUG.

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.

In 2019 is de RUG het aantal van 100 datalekken gepasseerd sinds de start van de registratie in 2016. Op grond van dit aantal inbreuken tekenen zich enkele contouren af. Zo zijn veel datalekken terug te herleiden tot verkeerde autorisaties. Ook is naar het inzicht van de FG bij de afhandeling van datalekken met een laag risicoprofiel[84] de betrokkenheid van het CvB niet essentieel.

In 2020 is op voordracht van de security manager en FG reeds gestart met een onderscheid in rapportage richting het CvB gebaseerd op het risicoprofiel van datalekken. De RUG dient deze nieuwe rapportagemethode en –lijnen te evalueren.

[83] Onder een datalek wordt ook het per ongeluk, maar definitief verwijderen van persoonsgegevens, het ongeautoriseerd wijzigen van persoonsgegevens of de verwerking zonder gerechtvaardigde grondslag geschaard.
[84] Datalekken met een laag risicoprofiel worden enkel intern geregistreerd maar worden in principe niet aan de Autoriteit Persoonsgegevens of de betrokkenen gemeld. Dit is in lijn met de wettelijke bepalingen daaromtrent.

Verder heeft het CvB naar aanleiding van voorgevallen datalekken concrete maatregelen voorgeschreven waardoor de kans op soortgelijke datalekken in de toekomst kleiner wordt. Dit zijn tevens maatregelen die structureel van aard zijn en bijdragen aan een privacybestendige organisatie. Ook wordt voorlichting naar aanleiding van datalekken vaker voorgeschreven.

Om verder te groeien op dit onderdeel, dient de RUG te kijken naar voorlichting en training van medewerkers. Die training of voorlichting dient vooral gericht te zijn op het identificeren van datalekken. Voor nieuwe medewerkers is de documentatie omtrent onboarding een optie.

Inventarisatie datalekken

In heel 2019 zijn er **30** beveiligingsincidenten[85] gemeld. Daarvan zijn er **15** als datalek gekwalificeerd en intern geregistreerd, van die 15 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[86] 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 2020 gestreefd worden naar het beheer van datalekken in een gecentraliseerd systeem.

De komende jaren zal het aantal gemelde datalekken gelijk blijven of zelfs groeien. Dit is grotendeels het gevolg van meer bewustwording en een grotere meldingsbereidheid.

Met de groei van het volwassenheidsniveau van de RUG, zal het aantal datalekken op lange termijn vrijwel zeker afnemen. Dit is het gevolg van meer passende technische en organisatorische maatregelen, zoals bewustwording bij medewerkers, heldere en eenduidige processen en betere (IT-)beveiliging.

Veel incidenten worden nu nog niet herkend en/of gemeld als inbreuk in verband met persoonsgegevens. Deze constatering is kenmerkend voor het domein onderzoek.

Datalekken in onderzoek

Vanuit het domein onderzoek is één datalek gemeld. Gezien het grote aantal[87] onderzoeken met persoonsgegevens lijkt dit niet te worden verklaard door excellente beveiliging, maar duidt vrijwel zeker op het gebrek aan kennis over datalekken en de melding ervan.

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.

[85] Dit zijn mogelijke datalekken; verder onderzoek bij de RUG wijst uit of een incident ook een datalek is.
[86] Er zijn datalekken gekwalificeerd waarbij UMCG, een studentenvereniging of derde de verantwoordelijke is.
[87] 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).

Bij de start van een onderzoek dient de onderzoeker en zijn team een datalek te kunnen identificeren. Bewustwording van onderzoekers over (het melden van) datalekken is daarom gewenst.[88] Een logische plek om hiermee te starten is de graduate school.

[88] 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

In 2019 heeft de RUG stappen gezet om haar privacymanagementorganisatie verder te laten groeien. Het instellingsbrede volwassenheidsniveau groeide van 1,3 naar 1,7. Voor een organisatie ter grootte van de RUG, met drie verschillende domeinen en duizenden verwerkingen is dat een nette stap. Dit is te danken aan de inzet van een groot aantal collega's.

Onder die collega's vallen onder andere de privacy- & securitycoördinatoren. Binnen alle domeinen hebben zij zich verenigd en werken zij toe naar uniforme processen. Dit moet in 2020 resulteren in de groei van het aantal helder omschreven processen in het register. Doelbinding, dataminimalisatie en passende beveiliging moeten binnen die processen op centraal niveau bewaakt worden.

Voor de (ondersteunende) diensten geldt dat zij in 2019 niet geheel aan de verwachtingen voldeden. In 2020 moeten zij aandacht besteden aan hun Werkplannen. Daarin dienen de verwerkingen met de hoogste risico's worden benoemd. Daarnaast is een realistische planning om de risico's te mitigeren vereist. Faculteiten moeten uiteindelijk kunnen vertrouwen op de verwerking van persoonsgegevens in de gefaciliteerde processen en systemen.

Binnen het domein onderzoek is meer aandacht nodig voor de ondersteuning van de onderzoeker. Bewustwording en kennis, maar ook praktische maatregelen zijn benodigd. Het vergroten van kennis is ook bij de facultaire ondersteuning en de ethische commissies noodzakelijk.

Naast de interne organisatie, is er meer contact met betrokkenen over de verwerking van hun persoonsgegevens. Het is studenten en medewerkers eenvoudiger gemaakt om persoonsgegevens op te vragen, te rectificeren en te verwijderen. Hierbij speelt een duidelijkere communicatie vanuit de RUG een rol.

Het voornemen om het gemiddelde volwassenheidsniveau op 2,0 te hebben in 2020 is te realiseren. Daarvoor blijft toewijding van het CvB, directies en faculteitsbesturen essentieel.

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.

© Centrum voor Informatiebeveiliging en Privacybescherming

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.

© Centrum voor Informatiebeveiliging en Privacybescherming

Bijlage 2. Compact model privacyverklaring RUG

rijksuniversiteit groningen

19-3-2020

Privacyverklaring Digitaal Studentendossier

De Rijksuniversiteit Groningen (RUG) gaat altijd zorgvuldig met uw persoonsgegevens om; u moet erop kunnen vertrouwen dat deze rechtmatig worden verwerkt en passend worden beschermd. De RUG wil daarom transparant zijn over wat zij doet met uw persoonsgegevens. Het beleid hiervoor is opgenomen in het document: Algemeen beleid bescherming persoonsgegevens rijksuniversiteit Groningen hierin kunt u in hoofdlijnen de visie en uitgangspunten van de RUG lezen. Daarnaast is er een Algemene Privacyverklaring. In deze verklaring wordt u geïnformeerd over de manier waarop de RUG uw gegevens verwerkt en welke rechten u heeft.

Wat is het doel van de verwerking:
Het opbouwen en onderhouden van het studentdossier

Wat is het brondocumenten en welke bewaartermijnen:
Gegevens worden aangeleverd via DUO
Wij bewaren uw gegevens conform wet- en regelgeving en met name volgens Selectielijst Universiteiten en UMC's van 1 jan 2020

Op welke grond verwerken wij uw gegevens:
Taak van Algemeen belang (Wet op hoger onderwijs en wetenschappelijk onderzoek)

Welke gegevens verwerken wij van u:
- Aanhef
- Titulatuur
- NAW-gegevens
- Geboortedatum, -plaats
- Contactgegevens
- Correspondentiegegevens
- Gezondheidsgegevens
- Vooropleidingsgegevens
- Studie-informatie

In welke systemen bewaren wij uw gegevens:
Uw gegevens worden bewaard in een aantal studie ondersteunende systemen zoals Progress en Nestor.

Wie ontvangen uw gegevens:
Uw gegevens worden binnen de RUG enkel met andere faculteiten gedeeld als dat noodzakelijk is voor het doel.

Welke rechten heeft u op grond van de AVG
- Te verzoeken om inzage, verwijdering of rectificatie van uw persoonsgegevens;
- Te verzoeken om de beperking van de verwerking van uw persoonsgegevens;
- Bezwaar te maken tegen de verwerking van uw persoonsgegevens.

Met wie kunt u contact opnemen:
U kunt met uw vragen en verzoeken over de verwerking van uw persoonsgegevens terecht bij:
Rijksuniversiteit Groningen
T.a.v. Centraal Loket Privacy
Postadres: Postbus 72
9700 AB Groningen
E-mail: privacy@rug.nl

Uw bericht wordt altijd gedeeld met de Functionaris voor de Gegevensbescherming van de RUG.