Jaarrapportage bescherming persoonsgegevens RUG 2020

Een vastgestelde handelwijze is nodig in crisistijd

Mr. A.R. Deenen
Functionaris voor de Gegevensbescherming

8 april 2021

Managementsamenvatting en conclusie

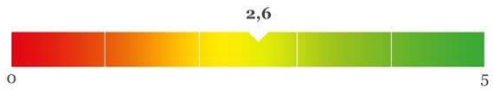
De Jaarrapportage Bescherming Persoonsgegevens RUG 2020 (“jaarrapport”) is geschreven voor het College van Bestuur van de RUG. Beschreven is hoe de RUG omgaat met de bescherming van persoonsgegevens in het jaar dat in het teken van de coronacrisis stond.

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. Hierbij ligt de focus op de hoogste risico’s en de daarbij voorgestelde maatregelen.

Verder wordt er in dit jaarrapport teruggekeken op 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 (op een schaal van 5,0). Voor 2020 scoort de RUG een 2,1. Dit betekent een verhoging ten opzichte van 2019 (1,7), maar geeft ook aan dat er nog een weg te gaan is. Voor de aankomende jaren is focus op risicomanagement belangrijk; de RUG handelt op dat vlak nog vaak reactief. De toename in volwassenheidsniveau die zich in dit jaarrapport aftekent is met name te danken aan een hoge mate van transparantie en zorgvuldige omgang met de rechten van betrokkenen. Ondanks de coronacrisis die de universiteit ook treft, blijft de opgebouwde organisatie tot nu toe intact.

Het volwassenheidsniveau van 2,1 voor 2020 is opgebouwd uit de volgende onderdelen:

Privacybeleid en inbedding in de organisatie:



in lijn met het privacybeleid hebben 15 van de 16 faculteiten en diensten werkplannen opgesteld waarin risico’s en maatregelen zijn beschreven. De vervolgstap bestaat uit het koppelen van (financiële) middelen aan de privacydoelstellingen.

Risicomanagement:

privacyrisico’s zijn nog onvoldoende in beeld; risico-inventarisaties (zoals Data Protection Impact Assessments) worden nauwelijks uitgevoerd en de structurele toepassing van “Privacy by Design” ontbreekt.

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 ontoereikend. Daarnaast wordt de FG in veel gevallen niet (tijdig) betrokken bij aangelegenheden die de bescherming van persoonsgegevens raken.

Register:

het register geeft niet het gewenste inzicht en overzicht van de actuele verwerkingen van persoonsgegevens. Toegewerkt wordt naar een overzicht van uniforme verwerkingen.

Kwaliteitsmanagement:

het niveau van kwaliteitsmanagement is binnen de RUG gelijk gebleven. Bewaking van de juistheid van de persoonsgegevens is niet standaard onderdeel van processen. Daarentegen is de omgang met wijzigingsverzoeken van betrokkenen goed.

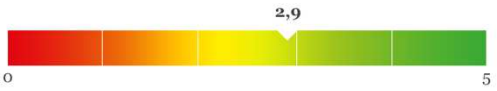
Bewaren van persoonsgegevens:

bewaartermijnen uit de Selectielijst worden toegepast en zijn onderdeel gemaakt van richtlijnen binnen de RUG. Toepassing van de richtlijnen is een belangrijke vervolgstap. Verder vraagt het “archief” in de e-mail, Y-schijf en Google Drive nog steeds aandacht.

Beveiligen van persoonsgegevens:

organisatiebreed bestaat een beveiligingsplan, maar deze is niet overal geïmplementeerd. Decentraal vinden nog onvoldoende risicoanalyses plaats en blijven veel maatregelen dus achterwege.

Informatieverstrekking en rechten betrokkenen:



voor de informatieverstrekking aan betrokkenen wordt organisatiebreed dezelfde standaard gehanteerd. Verder worden de verzoeken van betrokkenen tijdig en zorgvuldig afgehandeld.

Verwerkersovereenkomsten en doorgifte:

de RUG heeft met het merendeel van de verwerkers afspraken gemaakt. Controle op de naleving van de verwerkersovereenkomst aan de zijde van de verwerker vindt echter zelden plaats. Ook ontbreekt het de RUG nog aan een vastgestelde handelwijze omtrent internationale doorgifte.

Datalekken:

het aantal gemelde datalekken is vergeleken met 2019 gestegen (van 15 naar 43). De omgang met datalekken is onderdeel van richtlijnen en organisatiebrede communicatie. Binnen het domein onderzoek groeit nu ook langzaam de bewustwording omtrent datalekken.

Conclusie:

met de verdere inbedding van het privacybeleid in de organisatie heeft de RUG wederom een toename in het volwassenheidsniveau gerealiseerd. De omvang en structuur van de organisatie, maar ook de diversiteit van de taken maakt dat dit geen eenvoudige stap is geweest.

Naast de bestuurders en directies hebben de collega's als de privacy- & securitycoördinatoren veel werk verzet. De domeinen hebben zich verenigd en kunnen toewerken naar uniforme processen in 2021. Concrete plannen zijn gemaakt en zijn in 2021 gestart.

De (ondersteunende) diensten vragen net als in 2019 nog aandacht. In 2021 moeten zij aandacht besteden aan hun Werkplannen. Daarin dienen de verwerkingen met de hoogste risico's te worden benoemd. Ook een realistische planning is vereist om de risico's te mitigeren. Faculteiten moeten immers kunnen vertrouwen op de verwerking van persoonsgegevens in de gefaciliteerde processen en systemen.

Binnen het domein onderzoek is al meer aandacht voor de ondersteuning van de onderzoeker. Bewustwording en kennis, maar ook praktische maatregelen zijn nodig. Het GDCC[1] gaat hierin een belangrijke rol spelen.

Naast de interne organisatie, is er meer contact met betrokkenen over de verwerking van hun persoonsgegevens. De omgang met die betrokkenen heeft een (positieve) vlucht gemaakt.

Voor verdere groei is focus op risicomanagement en "privacy by design" zeer gewenst. Toewijding van het CvB, directies en faculteitsbesturen blijft daarbij essentieel.

[1] Groningen Digital Competence Center.

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);

CISO – de Chief Information Security Officer is verantwoordelijk voor het informatiebeveiligingsbeleid;

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 2020 (“jaarrapport”) voor het College van Bestuur van de RUG. Het jaarrapport is opgesteld door de Functionaris voor de Gegegevensbescherming (“FG”) van de RUG en heeft dezelfde structuur als voorgaande jaarrapportages. Het jaarrapport heeft als doel om te informeren, te signaleren en te adviseren.

De RUG is een grote en brede organisatie. In dit jaarrapport worden daarom de aspecten met het hoogste risico voor betrokkenen en de organisatie benoemd. Daarbij heeft de FG hulp gehad van onder meer de privacy- en securitycoördinatoren, het privacyteam (ABJZ), de CISO en de IT-auditor. Het jaarrapport is niet uitputtend bedoeld, maar is goed als leidraad te gebruiken voor het aankomende jaar.

In dit jaarrapport wordt teruggekeken naar het voorgaande jaar: een jaar dat werd gekenmerkt door een pandemie (COVID-19) en alle daarbij behorende gevolgen en in mindere mate naar de verwachtingen van het komend jaar. Gekeken wordt naar de voortgang en eventuele stagnatie in de ontwikkeling van de privacymanagementorganisatie. Er zijn onderdelen waarop de RUG geen vooruitgang heeft geboekt; een herhaling van eerder voorgestelde adviezen zien we daarom terug in dit jaarrapport.

2. Inleiding

Het afgelopen jaar heeft aangetoond dat (het gebrek aan) gegevensbescherming alle sectoren en werelddelen raakt.[2] Dit geldt ook voor alle drie domeinen binnen de RUG: onderwijs, onderzoek en bedrijfsvoering. Met de verschillende nationale en internationale incidenten (datalekken) wordt de bescherming van privacy meer evident. De bescherming van persoonsgegevens is niet langer een onderwerp voor enkel de privacy officers en juristen, maar hoort inmiddels thuis op de bestuurstafel.

Het aantal hackpogingen naar persoonsgegevens is afgelopen jaar sterk gestegen.[3] Gezien de impact van dat soort incidenten voelt het “digitale goud” voor veel organisaties eerder aan als lood. De RUG heeft het digitale goud steeds beter in het vizier. De volgende stap is het verder verbeteren van de omgang ermee.

Gebleken is dat het toewerken naar een zorgvuldige omgang met persoonsgegevens in de gehele keten van processen vraagt om implementatie van privacy by design. Dit vereist een organisatiebrede vastgestelde handelwijze. Zonder die gehanteerde handelwijze is de privacybescherming een sluitstuk en geen integraal onderdeel van het doen en laten van de RUG.

Wat het afgelopen jaar duidelijk heeft gemaakt is dat de RUG zich nog niet bevindt op het gewenste volwassenheidsniveau. Met de transitie naar een vorm van hybride onderwijs en werkplek wordt veelal reactief omgegaan met de bescherming van persoonsgegevens. In veel situaties ontbreekt een vastgestelde handelwijze om proactief te kunnen acteren. Dit wil echter niet zeggen dat alle methodieken, richtlijnen en beleidsstukken voor online onderwijs klaar hoeven te liggen. Wel vraagt de organisatie en de nieuwe situatie om de toepassing van privacy by design in het geval van nieuwe processen.

Ook moet geconstateerd worden dat 2020 het eerste jaar is na de inwerkingtreding van de AVG dat er geen project is gestart om tot een hoger volwassenheidsniveau te komen. Wel hebben de meeste privacy- en securitycoördinatoren (“P&S-coördinatoren”) namens de faculteitsbesturen en directies een nieuw werkplan Privacy & Security (“Werkplan”) opgesteld en aangeleverd.

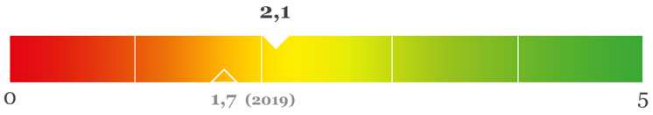
De Werkplannen volgen een jaarlijkse cyclus die aansluit op de bestuurlijke PDCA-cyclus. In het Werkplan staat beschreven hoe omgegaan wordt met de privacy en security in alle toepasselijke domeinen. De kern bestaat uit het identificeren van risico’s en het beschrijven van de mitigerende maatregelen. Eén van de manieren om risico’s in kaart te brengen is middels een DPIA[4]. Deze hebben plaatsgevonden en zijn landelijk gekend.[5]

---

[2] C. Véliz, C. Privacy and digital ethics after the pandemic. *Nature Electronics* 4, 10–11 (2021), 25 januari 2021.
[3] T. Borst, ‘Meldingen van hackpogingen persoonlijke data stijgen met 30 procent’, *NRC,* 1 maart 2021.
[4] Data Protection Impact Assessment.
[5] De DPIA’s “tentamens op afstand” en “Google G Suite for Education” zijn veel besproken binnen de onderwijs-sector, bij de Amsterdamse rechtszaak omtrent online proctoring en heeft zelfs het landelijke nieuws gehaald.

Bij het vaststellen van de volwassenheid van de privacymanagementorganisatie is wederom het CIP-model gehanteerd.[6]

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.



Kijkend naar 2020 kan geconcludeerd worden dat het algemene volwassenheidsniveau van de RUG inmiddels op niveau **2,1** ligt. In 2019 bevond de RUG zich nog op niveau 1,7. Ondanks de coronacrisis kent de RUG een groei.

Bij die groei van het volwassenheidsniveau is een toelichting op zijn plaats. De geconstateerde groei is veelal het resultaat van werkzaamheden in de jaren daaraan voorafgaand. Ook is het algemene volwassenheidsniveau van de RUG een ongewogen rekenkundig gemiddelde. In het geval van de RUG betekent dit dat er uiteenlopende niveaus zijn behaald op de tien onderdelen.

Voor de leesbaarheid van dit rapport is elk onderdeel beschreven in een eigen hoofdstuk. 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 (☑).

[6] M. Koers e.a. (red), 'Privacy Volwassenheidsmodel', *Centrum voor Informatiebeveiliging en Privacybescherming* 6 mei 2019, versie 3.2, cip-overheid.nl.

3. Privacybeleid en inbedding in de organisatie

Het afgelopen jaar werd de implementatie van de privacymanagementorganisatie overschaduwd door de coronacrisis en de gevolgen daarvan binnen onderwijs en onderzoek. Desondanks wil het CvB regie houden op de onderwerpen privacy en security. Ook stelden de meeste faculteiten en diensten tijdig een Werkplan op waarmee het beheer op privacy en security wordt beschreven.

Privacybeleid is binnen de RUG aanwezig op centraal niveau.[7] In lijn met dat beleid stellen de faculteiten op hun beurt richtlijnen op ten aanzien van de bescherming van persoonsgegevens in onderzoek. Voor onderwijs is sinds 2020 het organisatiebrede beleidsplan Domein Studenten en Onderwijs in gebruik.[8] Hierin wordt de omgang met persoonsgegevens beschreven binnen de levenscycli van de studenten en het onderwijs.

Bij de RUG wordt de effectiviteit van het privacybeleid momenteel niet gemeten. De Werkplannen kunnen meer inzicht geven in de effectiviteit van het privacybeleid en de inbedding in de organisatie (op decentraal niveau). Met andere woorden: bereikt de RUG haar doelen met het huidige privacybeleid? Voor alle drie domeinen is dat een actuele vraag.

Om als organisatie verder te groeien in haar volwassenheid doet de RUG er verstandig aan om heldere privacydoelstellingen te beschrijven en de benodigde middelen hieraan te koppelen.[9] Deze dienen op hun beurt terug te komen in de financiële cyclus van de RUG. Dit vraagt om toewijding van het management, op zowel centraal als decentraal niveau.

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 de kans dat persoonsgegevens in strijd met wet- en regelgeving worden verwerkt en het privacybeleid en relevante wet- en regelgeving ineffectief worden geïmplementeerd.

[7] Algemeen beleid bescherming persoonsgegevens Rijkuniversiteit Groningen.
[8] Dit beleidsstuk is tot stand gekomen in samenspraak met de privacy & securitycoördinatoren van de RUG.
[9] Dit geldt ook voor het budgetteren van trainingsprogramma's zoals de Workshop Data en Privacy of training vanuit de onderzoeksondersteuning. De eerste lijkt overigens definitief te eindigen in Q2 2021.

Sinds 2020 wil het CvB meer regie hebben op de borging van privacy en security op centraal niveau. Daarom kiest zij er voor meer bij te sturen op beleid en processen door de opzet van de Stuurgroep Privacy & Security, de periodieke evaluatie van de Roadmap informatiebeveiliging 2020-2021 ("Roadmap informatiebeveiliging") en borging van de voorgestelde maatregelen als gevolg van datalekken.

In het afgelopen jaar is de rol van de P&S-coördinatoren duidelijker geworden en worden zij door collega's vaker opgezocht. De P&S-coördinatoren delen onderling meer kennis en doen dat op een meer structurele wijze. Dit gebeurt binnen de drie zogenaamde platforms; één voor onderwijs, één voor onderzoek en één voor bedrijfsvoering; hierover later meer.

Borging privacybeleid en Werkplannen

In het Algemeen Beleid Bescherming Persoonsgegevens ("privacybeleid") is de governance inzake privacymanagement vastgelegd en vastgesteld. Hierin wordt de PDCA-cyclus beschreven die de privacymanagementprocessen moet borgen. De Werkplannen staan hierbij centraal. De universiteit hanteert voor het derde jaar op rij de Werkplannen Privacy & Security.

In het Werkplan zijn per faculteit of dienst de taken en verantwoordelijkheden beschreven. Daarnaast worden de verwerkingen met de hoogste risico's benoemd en zijn de maatregelen in een planning opgenomen. Binnen het Werkplan krijgen privacy én security een plek.

Wil de RUG de organieke inbedding verder vergroten, dan is de volgende stap om de planning van de benodigde middelen te koppelen aan de cyclus van de Werkplannen.

Faculteiten en diensten

De faculteitsbesturen en directies van de diensten hebben, ondersteund door de P&S-coördinator(en), in 2020 wederom de Werkplannen gepresenteerd. Deze bevatten doorgaans een duidelijke 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 CISO[10], de IT-auditor en de functionaris gegevensbescherming. Bij de beoordeling werden zij ondersteund door ABJZ.

Net als bij de Werkplannen van voorgaande jaren is de vorm en inhoud indicatief voor de inzet van de desbetreffende faculteit of dienst op dit thema. Zo zijn een deel van de datalekken te herleiden tot een gebrek aan implementatie van de beginselen. Denk aan beginselen als vertrouwelijkheid, opslagbeperking en dataminimalisatie.

De Werkplannen van de ondersteunende diensten vragen aankomend jaar extra aandacht. Zo is het Werkplan van het Bureau afgelopen jaar als onvoldoende beoordeeld.[11]

[10] Chief Information Security Officer.
[11] Er is geen Werkplan aangeleverd door de directie van het Bureau.

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[12]	●
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	●

Beoordeling Werkplannen diensten			
Facilitair bedrijf	●	Het Bureau	●
Centrum voor Informatie Technologie	●	Universiteitsbibliotheek	●

De medewerking van de diensten is onontbeerlijk om als universiteit tot een hoger volwassenheidsniveau te komen. Zij leveren 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.

Verder is per faculteit en dienst aandacht nodig voor de principes “Privacy by Design” en “Privacy by Default”. Deze principes vragen om het toepassen van privacyvriendelijke maatregelen bij het ontwerp van een dienst, product, project en/of verwerking. Dit is op centraal niveau tot nu toe niet beschreven en vastgesteld.

Specifiek in tijden van crisis is Privacy by Design cruciaal om de bescherming van persoonsgegevens te waarborgen. Er is niets verleidelijker om vanuit een financieel oogpunt of vanwege de snelheid te kiezen voor diensten en producten die geen tot minder bescherming van persoonsgegevens behelzen.[13] Het stellen van randvoorwaarden levert uiteindelijk meer (tijdswinst) op dan het achteraf herstellen van tekortkomingen.

De RUG dient op centraal niveau te komen tot maatregelen die het principe van “Privacy by Design” onderdeel maken van (nieuwe) processen waarbij persoonsgegevens worden verwerkt. Beslissingen in crisistijd hebben namelijk ook impact op de processen na de crisis.

[12] 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.
[13] Zo zijn AFAS (bedrijfsvoering) en Gather.Town (onderwijs) in gebruik genomen terwijl deze op dat moment niet voldeden aan de vereisten van de AVG.

Drie domeinen, drie platforms

Sinds twee jaar kent de RUG drie platforms voor de P&S-coördinatoren; voor elk domein één.

Binnen een platform stemmen de P&S-coördinatoren van het specifieke domein zaken af ten aanzien van de zorgvuldige omgang met persoonsgegevens. De basis voor richtlijnen, (beveiligings)maatregelen en acties wordt hier gelegd.

De coördinatoren zijn verantwoordelijk voor de inventarisatie van alle verwerkingen binnen de eigen faculteit/dienst, maar ook voor het initiëren van Data Protection Impact Assessments ("DPIA's") en beantwoording van vragen over privacy en security van collega's.

Per domein volgt hierna de staat van de privacymanagement(organisatie).

Privacy en onderwijs

In 2020 is het beleidsplan Studenten en Onderwijs[14] organisatiebreed vastgesteld. Het beleidsplan geeft invulling aan de zogenaamde privacybeginselen[15] binnen het domein onderwijs en de onderwijsadministratie. Deze zijn in begrijpelijke taal uiteengezet.

Sinds de vaststelling van het CvB zijn de richtlijnen binnen het beleidsplan niet tot nauwelijks geïmplementeerd in de onderwijsprocessen. Hier zijn een aantal verklaringen voor te vinden:

1) het beleidsplan spreekt van een "proceseigenaar" die verantwoordelijk is voor de toepassing van de richtlijnen. Het aanwijzen van één proceseigenaar voor specifieke verwerkingen is binnen de RUG niet altijd mogelijk vanwege meerdere stakeholders.
2) Proceseigenaren zijn niet bekend met het beleidsplan Studenten en Onderwijs.
3) De coronacrisis heeft veel gevraagd van het ondersteunend personeel met als gevolg dat veilig(er) of zorgvuldig(er) omgaan met persoonsgegevens niet altijd de hoogste prioriteit krijgt.

Bij diverse 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 is geborgd.

Taken en verantwoordelijkheden dienen naar aanleiding van het beleidsplan Studenten en Onderwijs verduidelijkt te worden. Logischerwijs is dit een onderdeel van de evaluatie van het beleidsplan Studenten en Onderwijs.

[14] 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.
[15] De privacybeginselen worden gevonden in artikel 5 AVG.

Docenten en onderwijsadministratie

Docenten, het personeel bij de onderwijsadministraties en de studieadviseurs hebben het meeste contact met studenten. Zij verwerken binnen het onderwijs dan ook het merendeel van alle persoonsgegevens.

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. Aansluiting kan daarbij gezocht worden bij de training van de Teaching Assistants of de Workshop Data en Privacy.

Het uiteindelijke doel is deze medewerkers bekend te maken met enkele beginselen en ze handvatten te geven om incidenten te signaleren en/of kennis te laten maken met de P&S-coördinator en de Privacy Portal.[16]

Verwerking persoonsgegevens door studenten

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

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

Studenten die onderzoek doen met persoonsgegevens zijn zich doorgaans niet bewust van de noodzakelijke technische en organisatorische maatregelen die nodig zijn om persoonsgegevens zorgvuldig te verwerken. Hetzelfde geldt voor de begeleider.

Het vergroten van bewustwording en kennis bij de onderzoekende student is nodig om te komen tot zorgvuldige verwerkingen van persoonsgegevens. De kennis van de student hoeft minder uitgebreid te zijn wanneer een veilige infrastructuur wordt geboden. Dergelijke infrastructuur heeft namelijk al veel waarborgen ingebed.

Afhankelijk van de omvang en het soort onderzoek is er binnen de universiteit al veel relevant en bruikbaar materiaal aanwezig. Voor bewustwording en training vormt de e-learning “Privacy in research: asking the right questions” een sterke basis.[17]

[16] De Privacy Portal bevat veelgestelde vragen, standaardmodellen, contactinformatie van de P&S-coördinatoren en het CERT-team. De laatste is relevant bij het melden van (mogelijke) datalekken.

[17] De e-learning en ander materiaal 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. De e-learning is een van de resultaten uit de toegekende Comenius Senior Teaching Fellowship.

Onderzoek en persoonsgegevens

Binnen het onderzoeksdomein is binnen de faculteiten nog behoefte aan meer duidelijk beschreven taken, verantwoordelijkheden en bevoegdheden.

Dit kan onder meer beschreven worden middels een RASCI-model.[18] Beter specificeren wie binnen het onderzoek welke taak en verantwoordelijkheid heeft voorkomt onderlinge wrijving tussen stakeholders in onderzoek. Hieronder vallen ook de verwerkers en onderzoeksfinanciers.

Gezien de vrijheid die faculteiten toekomt voor wat betreft onderzoek, is een bottom-up-benadering verstandig. Start binnen de faculteiten met het beschrijven van taken, verantwoordelijkheden en bevoegdheden. Het CvB kan daarna de 'best practices' belichten en het raamwerk voor de taken, verantwoordelijkheden en bevoegdheden formeel vastleggen.

Met name op het gebied van onderzoek en ondersteuning is duidelijkheid over de verdeling van verantwoordelijkheden een belangrijk aandachtspunt. De ethische commissie, datastewards, P&S-coördinatoren, de FG, decanen en de graduate schools zijn allen betrokken en hebben een rol. Hierbij is overlap, maar zijn ook hiaten zichtbaar.

De onderzoeker en de AVG

Per jaar vinden er binnen de RUG meer dan duizend onderzoeken plaats met persoonsgegevens. Het privacybeleid beschrijft taken, verantwoordelijkheden en bevoegdheden op hoofdlijnen. Op detailniveau bestaat er dus nog onduidelijkheid.

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.

Bij onderzoek gaat het om een gedeelde verantwoordelijkheid. Op centraal en decentraal niveau dient verantwoord onderzoek te worden gefaciliteerd met bijvoorbeeld richtlijnen omtrent de invulling van de beginselen, maar ook met technische maatregelen.

De wijze waarop ondersteuning van 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 uiteen.[19]

Ook de rol van de ethische commissie bij de toetsing op de beginselen van de AVG is niet geconcretiseerd. De ethische commissies die de AVG-beginselen wel meenemen in de (ethische) toetsing bezitten niet altijd voldoende kennis om effectief te toetsen.[20]

---

[18] https://nl.wikipedia.org/wiki/RACI-model.
[19] 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).
[20] Het kan hierbij gaan om basale kennis over definities als "persoonsgegevens" of "pseudonimisering".

Om de onderzoeker voldoende te kunnen ondersteunen is degelijke inrichting en kennis bij de facultaire onderzoeksondersteuning noodzakelijk.[21] Periodieke training van het ondersteunend personeel is daarom gewenst. Een voorbeeld vormt de kennisuitwisseling tussen de leden van de ethische commissies.

Wat betreft de centrale ondersteuning van onderzoek ondergaat de RUG haar derde transitie in een korte periode.[22] Vanuit de centrale organisatie gaat het Groningen Digital Competence Center ("GDCC") ondersteuning bieden aan onderzoekers die vragen hebben over verwerking van persoonsgegevens. De RUG ontving hiervoor impulsfinanciering.[23] Het GDCC brengt relevante kennis, technische middelen en bruikbare 'best practices' samen. Het zet de product- en dienstcatalogus van het RDO[24] door en creëert een loket voor onderzoeks-IT.

De verantwoordelijkheden en taken van het GDCC zijn nog niet uitgekristalliseerd. Dat dient in 2021 te gebeuren. Vormen van een duidelijk ingang voor onderzoekers heeft de aandacht.

Neem het GDCC en haar taken en verantwoordelijkheden op in het bestuurs- en beheersreglement van de Rijksuniversiteit Groningen.

Projectfinanciering voor het GDCC is voor twee jaar begroot en vastgesteld. Het opnemen van GDCC in de staande organisatie dient tijdig en goed uitgedacht te worden. Het huidige RDO en daarmee die ondersteuning houdt op te bestaan. Het verlies van expertise en ondersteuning ligt op de loer en is voor de RUG niet nieuw.[25]

Met de oprichting van het GDCC ligt de focus op (lokale) datastewards en de stimulering van interuniversitaire DCC's bij uitwisseling en dataopslag volgens de FAIR-principes[26].

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.

Research Datamanagementplannen

Naast de inrichting van het GDCC en de inzet van datastewards 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

[21] Wetenschap over 'building blocks' en onderzoekscenario's valt hier ook onder. Meer hierover in hoofdstuk 9.
[22] Tussen 2013-2016 stond het RDO centraal en van 2016-2018 was dat het programma Human Subject Research.
[23] Groningen Digital Competence Center ontvangt startsubsidie NWO, https://www.rug.nl/society-business/centre-for-information-technology/news/startsubsidie-nwo-gdcc, 25 januari 2021.
[24] Research Data Office.
[25] Concrete plannen voor de inrichting van het RDO ontbraken wat in 2019-2020 resulteerde in het wegvloeien van essentiële expertise over het toepassen van privacy in onderzoek.
[26] 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.[27]

Een onderdeel van de data lifecycle is de publicatie van data. Voor wat betreft de datasets die door onderzoekers van de RUG worden gepubliceerd in DataverseNL, vindt een controle plaats op de herleidbaarheid van de data. Met andere woorden: zijn individuele personen herleidbaar? Zo ja, dan kan de onderzoeker geadviseerd worden om te hercoderen, classificeren, bepaalde variabelen te verwijderen uit de dataset (mits dat wetenschappelijk verantwoord is) of het niet open maar restrictief opnemen van de dataset in de DataverseNL.

Binnen de andere repositories vindt een dergelijke controle op de datasets van onderzoekers van de RUG niet plaats, tenzij de onderzoeker dit expliciet verzoekt.

Een aanzienlijke kans bestaat dat individuele personen derhalve herleidbaar zijn in “open” gepubliceerde datasets, terwijl dit in beginsel een onrechtmatige verwerking van persoonsgegevens oplevert.

Om de bescherming van persoonsgegevens effectief te borgen bij publicatie van onderzoeksdata is het aan te raden om: 1) aandacht te besteden aan de herleidbaarheid van gegevens in het (format) datamanagementplan. Dit vereist kennis bij de onderzoeker, maar ook bij de ethische commissie en/of de datasteward. 2) Steekproefsgewijs te controleren op datasets in andere repositories.

Bedrijfsvoering en persoonsgegevens

Bij de RUG verwerken alle circa 6.000 medewerkers persoonsgegevens. Zoals bij veel bedrijfsprocessen begint ook zorgvuldige verwerking met het gezonde verstand van die medewerkers. Daarom hoeft niet iedereen een privacyprofessional te worden. Het kennen van de kaders en weten wanneer een P&S-coördinator geraadpleegd moet worden juist wel.

Bij de indiensttreding vindt “onboarding” plaats. Om structureel kennis binnen de organisatie te vergroten is toevoeging van de Workshop Data en Privacy (AVG) aan de onboarding sterk aan te raden.[28]

Naast de onboarding is binnen de HR-cyclus de wijziging van functie en/of locatie van een medewerker ook relevant. Aan een medewerker is een veelheid van autorisaties gekoppeld binnen een groot aantal systemen en diensten. Bij een mutatie van de functie of rol is aandacht voor een nauwkeurige wijziging of verwijdering van die autorisaties nodig.

De controle op het tijdig ontnemen van rollen en rechten is summier en wordt doorgaans niet volledig uitgevoerd.[29] Dergelijke situaties leiden al snel tot datalekken.[30] Zo blijken F-accounts jaren na vertrek van een medewerker nog toegankelijk met hetzelfde wachtwoord.

[27] Deze uitkomsten volgen uit de Research Data Management Audit 2018-2019 bij de RUG.
[28] Dit vindt ook plaats bij andere universiteiten zoals de Erasmus Universiteit Rotterdam.
[29] De trage of beperkte aanlevering van autorisatieoverzichten door het CIT werpt tevens een extra drempel op.
[30] De RUG kent in 2020 enkel datalekken die het gevolg zijn van het onterecht ongewijzigd laten van autorisaties.

Voor (grote) systemen en diensten 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.

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

Informatiebeveiliging organisatiebreed

Sinds 2020 is op centraal niveau meer regie op informatiemanagement en –beveiliging. De volgende wijzigingen hebben plaatsgevonden binnen de RUG.

Allereerst is een Chief Information Security Officer (CISO) aangewezen. Hij heeft in 2020 een organisatiebreed plan geschreven voor het vergroten van de informatiebeveiliging. De voortgang van de Roadmap informatiebeveiliging wordt elk kwartaal door het CvB besproken met de stakeholders. De CISO acteert verder onafhankelijk van (de directie van) het CIT, wat gebruikelijk is.[31]

Ten tweede is de Stuurgroep Privacy en Security in het leven geroepen waar ook één van de leden van het CvB plaatsneemt. Meer hierover in hoofdstuk 5 Doelbinding en intern toezicht.

Ten derde heeft informatiebeveiliging een prominentere rol gekregen in de Werkplannen en wordt ook de decentrale behoefte voor centrale informatiebeveiliging opgehaald.

Als laatste worden incidenten en datalekken elk kwartaal doorgesproken en de al dan niet genomen maatregelen beoordeeld. Dit wordt in hoofdstuk 12 Datalekken verder uiteengezet.

Informatiemanagement en vraagbundeling

Naast informatiebeveiliging is informatiemanagement een punt van aandacht. Waar voorheen de onafhankelijke eenheid RIO[32] organisatiebreed adviseerde over vraagarticulatie en -bundeling, is RIO nu BIC (Business Information Consultancy) en ondergebracht bij het CIT. Het CIT beheert daardoor echter vraag en aanbod. Dit leidt niet per se tot de meest wenselijke oplossingen voor de RUG en hierdoor wordt onder meer "privacy by design" niet standaard meegenomen. Om het beheer van vraag en aanbod te scheiden is het IVB-Board[33] in het leven geroepen. De focus van het board lijkt te liggen op bedrijfsvoering en minder op onderzoek.

Borg de onafhankelijkheid van informatiemanagement binnen de RUG. Versterk verder de betrokkenheid van het onderzoeksdomein binnen het IVB-Board.

[31] Position Paper: Inrichting governance van cybersecurity in het hoger onderwijs. Pas toe of leg uit!, Platform Integrale Veiligheid Hoger Onderwijs / KPMG, 20 april 2020.
[32] RUG Information Office was tot het einde van 2020 onderdeel van het Bureau van de RUG.
[33] Het Informatievoorziening Bedrijfsvoering Board bestaat uit vertegenwoordiging van de PH Middelen en de directeuren Finance & Control, HR en CIT. Het Board legt verantwoording af aan het Managementberaad en bepaalt de prioriteiten van de projecten informatievoorziening. Die prioriteiten zijn leidend voor het werk van BIC.

4. Risicomanagement

Om privacyrisico's effectief te mitigeren is een doorlopend proces vereist. Dit proces bestaat uit het signaleren en beoordelen van risico's en daarna het bewaken van de inzet van maatregelen. Dit begint al bij het ontwerp van processen en bij de aanschaf en ontwikkeling van diensten en producten. Het DPIA is een belangrijk instrument voor de analyse van risico's; 2020 kende een aantal interessante DPIA's en uitkomsten.

Allereerst is de RUG in de afgelopen twee jaren niet gegroeid op het onderdeel "risicomanagement" en schiet hier nog tekort. Risicomanagement is binnen de RUG nog een vrij reactief proces. De Werkplannen van faculteiten/diensten signaleren wel risico's, maar niet altijd de hoge risico's en/of in een (te) laat stadium.[34] Ook zijn veel risico's binnen de bedrijfsvoering niet in kaart gebracht; het helpt dan niet dat het Bureau geen Werkplan heeft.

Om risicomanagement op een hoger plan te brengen is het tijdig toepassen van Privacy by Design een belangrijke stap. Daarnaast vraagt de inzet van nieuwe technieken en/of diensten om het uitvoeren van een Data Protection Impact Assessment ("DPIA") indien de voorgenomen verwerking een hoog risico kan opleveren voor betrokkenen of de RUG.

Concreet betekent dit dat bij het ontwerpen en ontwikkelen van nieuwe processen de beginselen uit de AVG meegenomen worden (Privacy by Design). In het verlengde daarvan ligt de verplichting om in specifieke situaties ook een DPIA uit te voeren. De RUG kent enkele voorbeelden van verwerkingen in 2020 waarbij een DPIA vooraf verplicht was.[35]

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.

Kennis van het implementeren van risicomanagement is binnen de RUG aanwezig en wordt binnen decentrale eenheden reeds toegepast. Op basis van de Werkplannen uit 2020 zijn er meerdere faculteiten en diensten die het risicomanagement hebben beschreven en

[34] Werkplannen worden eenmaal per jaar opgesteld. Nieuwe processen wachten meestal niet op de nieuwe cyclus van de Werkplannen.
[35] De verwerking van persoonsgegevens bij het testen van studenten en medewerkers binnen de coronateststraat, maar ook de inzet van online proctoring bij online tentamens zijn duidelijke voorbeelden.

toegepast.[36] Zij beschrijven binnen alle domeinen de risico's en weten deze op een planmatige wijze te mitigeren. Daarentegen vindt het tijdig uitvoeren en/of plannen van DPIA's slechts bij enkele faculteiten plaats. Daarbij komt ook dat het centrale privacyteam onvoldoende capaciteit heeft om te assisteren bij het uitvoeren van alle DPIA's.[37]

Het Bureau en het CIT staan binnen de domeinen onderwijs en bedrijfsvoering vaak aan de wieg van nieuwe verwerkingen van persoonsgegevens. Bij beide diensten ontbreekt echter een structurele toepassing van het principe "Privacy by Design" en het uitvoeren van DPIA's.

Hierdoor blijft risicomanagement een reactief proces waarbij de betrokken P&S-coördinatoren en de leden van het (centrale) privacyteam onder hoge (tijds)druk herstelwerkzaamheden moeten uitvoeren wanneer nieuwe processen geïnitieerd worden.[38]

Structurele risico-inventarisaties en in het verlengde daarvan het DPIA, dienen binnen de faculteiten en diensten onderdeel van de reguliere bedrijfsvoering te worden. De RUG kent reeds een universiteitsbreed DPIA-protocol.[39]
Vergroot verder de kennis van het protocol bij faculteitsbestuurders, directies, P&S-coördinatoren en projectmanagers; bij de projectaanvraag kan Privacy by Design namelijk al worden toegepast.
Als laatste kan het CvB tijdens het besluitvormingstraject aansturen op een DPIA.

Naast de bedrijfsvoering wordt binnen het onderzoek steeds vaker een DPIA uitgevoerd nadat RDO of ABJZ de onderzoeker of onderzoeksgroep dit adviseert. Binnen onderzoek heeft dit meermalen geleid tot een helderdere formulering van het onderzoek (voor onderzoeksdeelnemers) en zijn veel risico's relatief eenvoudig verkleind of weggenomen.

Een positieve noot: de DPIA's die de universiteit uitvoert en beschrijft zijn kwalitatief van hoog niveau. Dit is onder meer bevestigd door de behandelende inspecteurs van de Autoriteit Persoonsgegevens bij het DPIA "tentamens op afstand". De DPIA-rapportages van de RUG worden dan ook veelvuldig gedeeld en gebruikt in de sector.

Binnen de eigen instelling mogen de uitkomsten van de DPIA's nog beter vindbaar worden gemaakt en de uitkomsten beter worden verspreid. Hiermee wordt "dubbel werk" voorkomen en worden (wetenschappelijke) collega's geholpen met de uitkomsten en/of voorgestelde oplossingen.

[36] Hierbij kan gedacht worden aan de Faculty of Science and Engineering, Faculteit Economie en Bedrijfskunde, Faculteit Ruimtelijke Wetenschappen, Faculteit Godgeleerdheid en Godsdienstwetenschap en de Universiteitsbibliotheek.
[37] Het centrale privacyteam kent twee personen die kunnen assisteren bij het opzetten en uitwerken van een DPIA.
[38] Illustratief zijn de verwerkingen van persoonsgegevens binnen de coronateststraat van de RUG en de inzet van online proctoring.
[39] College van Bestuur van de Rijksuniversiteit Groningen, DPIA-Protocol Rijksuniversiteit Groningen, 23 mei 2019.

Privacy by design

Een meer preventieve werkwijze heeft binnen de RUG de voorkeur. Door toepassing van het (wettelijk vastgelegde) beginsel van “privacy by design”[40] worden privacy en security tijdig betrokken; bij de vormgeving van processen en systemen.

Privacy by Design dient aan bod te komen bij de ontwikkeling of uitvraag van nieuwe applicaties/diensten waarbij persoonsgegevens zijn betrokken. Logische plekken voor de inbedding hiervan wordt gevonden in de (aanbestedings- en ontwikkel)processen van het CIT, het Bureau (O&O)[41], het Demand Management en het Facilitair Bedrijf.

Onderzoek(ers)

Vanuit het perspectief “risicomanagement” kent het onderzoeksdomein binnen de RUG slechts enkele wijzigingen. Ter implementatie van de zorgplichten uit de gedragscode WI[42] hebben de ethische commissies zich verenigd en wordt onderling kennis gedeeld. Hieronder valt ook de kennis over privacy en security. Waar het ethische commissies aan relevante kennis ontbreekt om privacy- en securityrisico’s te kunnen aanwijzen, wordt deze steeds vaker aangevuld.[43]

Het exacte aantal onderzoeken met persoonsgegevens, hoe deze onderzoeken worden uitgevoerd en waar het onderzoek plaatsvindt is deels onbekend.[44] De RUG kan derhalve niet voldoen aan haar verantwoordingsplicht.

Het vergroten van kennis bij de onderzoeker en de structurele inzet van de Research Portal (niet zijnde research.rug.nl) brengt het onderzoek en de daarbij behorende risico’s eerder in kaart. Helderheid per faculteit over de rol van de ethische commissies, GDCC en datastewards op het gebied van risicomanagement is een volgende stap om te komen tot een betere opzet van risicomanagement binnen onderzoek.

Opvolging DPIA WhatsApp

WhatsApp is begin 2021 wereldwijd in opspraak geraakt wegens de wijziging van haar voorwaarden.[45] Binnen de RUG wordt WhatsApp veelvuldig gebruikt binnen de bedrijfsvoering, maar ook binnen het onderwijs.[46] Dit geldt voor alle niveaus in de organisatie, het CvB inbegrepen.[47]

---

[40] 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.
[41] De Strategieafdeling Onderwijs & Onderzoek.
[42] De Nederlandse gedragscode wetenschappelijke integriteit 2018.
[43] Een aantal ethische commissies is aangevuld met, of winnen advies in bij, de P&S-coördinator van de faculteit.
[44] Meer hierover in hoofdstuk 6. Register.
[45] De voorgestelde wijzigingen van de voorwaarden van Whatsapp (Facebook) zijn niet van toepassing op de inwoners van de Europese Economische Ruimte, omdat deze dan in strijd met de AVG zouden zijn.
[46] Contact tussen docenten en studenten vindt onder meer plaats via Whatsapp.
[47] Dit ondanks het interne advies aan alle medewerkers om géén Whatsapp te gebruiken, maar een alternatief zoals Signal.

In november 2019 heeft de RUG reeds een DPIA uitgevoerd op zogenaamde messaging applicaties (apps). De uitkomsten zijn binnen hetzelfde DPIA ook toegepast op WhatsApp. De resultaten hiervan zijn op 12 december 2019 gepubliceerd.

Gebleken is dat er grote uitdagingen (risico's) bestaan bij gebruik van messaging apps en in het bijzonder WhatsApp als onderdeel van de bedrijfsvoering van de RUG.

De belangrijkste bevindingen waren:

1. duidelijke vereisten voor de leverancier en de technologie ontbreken binnen de RUG;
2. beleid ontbreekt omtrent het 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.[48]

Sinds de voorgaande uitkomsten is gekeken naar alternatieve applicaties. De zoektocht is na enkele maanden een stille dood gestorven. Ondertussen heeft de Autoriteit Persoonsgegevens data gepubliceerd over veelgebruikte applicaties waarbij er goede alternatieven zijn aan te wijzen voor Whatsapp.[49]

- Voorzie in een privacyvriendelijk alternatief voor het versleuteld chatten binnen de domeinen bedrijfsvoering en onderwijs, gebaseerd op de eisen uit het DPIA.
- Stel beleid op omtrent het gebruik van messaging apps.
- Wijs personeel op goed ingerichte alternatieven alvorens specifieke apps te ontmoedigen.

Niet onbelangrijk: geef als College van Bestuur het goede voorbeeld en hanteer een meer privacyvriendelijk alternatief voor Whatsapp. Dit advies ziet enkel op het gebruik van Whatsapp voor werkgerelateerde communicatie. Andersoortige (privé)communicatie valt in principe niet onder de verantwoordelijkheid van de RUG.

DPIA G Suite for Education

Dit DPIA heeft de onderwijswereld wakker geschud. Naast dat dit DPIA grote consequenties heeft voor de bedrijfsvoering van de RUG, heeft het ook consequenties voor het primaire en voortgezet onderwijs in Nederland.

Sinds 2014 wordt binnen alle domeinen van de RUG gebruik gemaakt van G Suite for Education ("G Suite")[50]. G Suite bestaat uit een reeks online toepassingen waaronder Gmail, Calendar, Drive en Docs. G Suite vormt bij de RUG onderdeel van honderden verwerkingen waarbij persoonsgegevens zijn betrokkenen. Denk daarbij aan het verwerken van

[48] In het geval van WhatsApp kan gedacht worden aan strijd met de volgende beginselen: rechtmatigheid, dataminimalisatie, opslagbeperking, transparantie en beveiliging.
[49] Keuzehulp privacy videobellen, Autoriteit Persoonsgegevens, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/keuzehulp_privacy_en_videobellen.pdf, versie 3, augustus 2020.
[50] Google hanteert sinds 17 februari 2021 een nieuwe naam: Google Workspace for Education.

persoonsgegevens zoals die letterlijk in een e-mailbericht zijn opgenomen, maar ook de metadata over het gebruik van de toepassingen door RUG-medewerkers, -studenten en derden.

In 2019 hebben de RUG en de Hogeschool van Amsterdam ("HvA") gezamenlijk opdracht gegeven aan Privacy Company om een DPIA uit te voeren op G Suite. Hierbij is begonnen met een juridische analyse van alle overeenkomsten inclusief voorwaarden die de RUG met Google heeft gesloten. Het vervolg bestond uit een technisch onderzoek en ving aan in 2020.

Eind 2020 zijn de eerste conceptresultaten van het DPIA door Privacy Company gepresenteerd aan de RUG en de HvA. Duidelijk werd dat er een aantal hoge en lage risico's voor de rechten en vrijheden van betrokkenen voortvloeiden uit het gebruik van G Suite. Deze geconstateerde risico's zijn door de Rijksoverheid aan Google voorgelegd.[51]

Google heeft naar aanleiding van de geconstateerde risico's een klein deel van de risico's weggenomen of is overeengekomen om dat op termijn te doen. De meerderheid van de hoge en lage risico's blijft echter bestaan.

De belangrijkste resterende (hoge) risico's zijn in het kort:

- Google heeft in de onderhandelingen vastgelegd dat zij de inhoudelijke gegevens nog maar voor drie doelen verwerkt. Toch wil Google niet uitsluiten dat zij zelf besluiten neemt om "Inhoudelijke gegevens" verder te verwerken, bijvoorbeeld voor de bestrijding van illegale activiteiten. Google weigert om alleen strikt noodzakelijke (proportionele) verwerkingen te doen.
- Google heeft een 17-tal vage doelen beschreven voor de verwerking van "Diagnostische gegevens", welke Google ook nog op elk moment kan wijzigen.
- Er is een gebrek aan transparantie ten aanzien van "Inhoudelijke gegevens" en "Diagnostische gegevens". Hoewel Google inmiddels handleidingen heeft gepubliceerd die wat meer duidelijkheid geven, is er geen overzicht van de doelen en persoonsgegevens, en kunnen beheerders en gebruikers een groot deel van de diagnostische gegevens niet bekijken. Daardoor is het onbekend of praktisch onmogelijk om te kunnen controleren of de verwerkingen van Google noodzakelijk zijn en voldoen aan de evenredigheidseisen.
- Bij de verwerking van "Diagnostische gegevens" geeft Google geen informatie over bewaartermijnen en de eventuele inzet van subverwerkers, omdat Google zichzelf als exclusieve verantwoordelijke ziet, en vindt dat zij hierover geen verantwoording hoeft af te leggen aan haar klanten.
- Voor een deel van de verwerkingen ontbreekt een grondslag voor Google en de RUG. Het betreffen vooral verwerkingen buiten de zogenaamde "Core Services"; alle verwerkingen waarvoor Google zichzelf als (enige) verantwoordelijke ziet. De RUG verstrekt in die gevallen feitelijk persoonsgegevens aan een derde partij buiten de EU, waarmee zij géén contractuele relatie heeft als verwerker of als gezamenlijke verantwoordelijke.

[51] Parallel aan het DPIA-traject liep er vanuit de Rijksoverheid ook een DPIA op G Suite (Enterprise). De RUG en HvA hebben (met ondersteuning van SURF) meegelift op de onderhandelingen tussen de Rijksoverheid en Google.

- Voor beheerders en gebruikers zijn er geen of te weinig "privacycontrolemogelijkheiden" om telemetrie en de Feedback module te kunnen beperken.
- Het is niet mogelijk gebleken om de rechten van de betrokkenen uit te oefenen. Google was niet bereid om inzage te geven in de persoonsgegevens van een van de betrokkene.

Een belangrijke vervolgstap vanuit de Rijksoverheid bestaat uit een zogenaamde voorafgaande raadpleging[52] bij de Autoriteit Persoonsgegevens ("AP"). Daarbij worden hoge risico's uit het DPIA voorgelegd aan de AP waarna zij schriftelijk advies uitbrengt.[53] Naast het advies kan de AP ook gebruik maken van een reeks andere bevoegdheden[54] waaronder, maar niet beperkt tot: verder onderzoek, het geven van een waarschuwing, gelasten een verwerking in lijn te brengen met de AVG en het opleggen van een verwerkingsbeperking-/verbod.

Namens de hele onderwijssector dienen SURF en Sivon een adviesaanvraag in bij de Autoriteit Persoonsgegevens ("AP") als antwoord op de resultaten uit het DPIA. Naar aanleiding van de uitkomsten van het DPIA en de adviesvraag bij de AP, is het uitdrukkelijke advies aan de RUG om een aantal zaken voor te bereiden en (direct) uit te voeren:

- het informeren van de betrokkenen over de huidige risico's binnen G Suite for Education in begrijpelijke taal;
- in afwachting van het advies van de AP de gevolgen van de hoge risico's voor de verschillende domeinen in kaart brengen;
- Google verzoeken om alle data te wissen die zij heeft vergaard op basis van de onrechtmatige toestemming voor de Additional Services, Feedback, zowel de diagnostische als de inhoudelijke gegevens;
- centraal de Additional Services blokkeren, het verkeer naar Google consumentenaccounts blokkeren (wanneer al is ingelogd met een RUG-account) en de Chrome Enhanced Spellcheck blokkeren;[55]
- binnen het onderzoeksdomein helder formuleren welke (privacyvriendelijke) alternatieven er zijn om onderzoek in overeenstemming met de AVG te kunnen uitvoeren. Dit is ook relevant bij het voldoen aan de eisen van de stakeholders van onderzoek, waaronder die van de (Europese) onderzoeksfinanciers;
- uitwerken van de verschillende toekomstscenario's vanwege de omvang en verwevenheid van G Suite binnen de RUG en het mogelijke advies van de AP.[56]

Naast de voorgestelde maatregelen, heeft de RUG ook een meer strategisch vraagstuk te beantwoorden. Hoe wil zij namelijk in de toekomst omgaan met (grote) techbedrijven en waar gaan de persoonsgegevens heen? Meer hierover in hoofdstuk 11.

---

[52] Details over de voorafgaande raadpleging zijn terug te vinden in artikel 36 AVG.
[53] Het advies van de Autoriteit Persoonsgegevens wordt halverwege mei 2021 verwacht.
[54] Zie artikel 36 juncto 58 AVG.
[55] Dit licht Google toe op de hulppagina's voor admins: https://support.google.com/a/answer/1668854?hl=en en https://support.google.com/chrome/a/answer/2657289?hl=en#spell_check_service_enabled.
[56] De AP kan adviseren om de verwerking van persoonsgegevens met G Suite for Education (op termijn) te staken vanwege strijdigheden met de AVG.

5. Doelbinding en intern toezicht

Elke verwerking van persoonsgegevens heeft een doel. Dit doel wordt vastgelegd en de RUG waakt ervoor dat persoonsgegevens niet voor andere doelen worden gebruikt dan waarvoor de persoonsgegevens initieel zijn verzameld. Het toezien op dit beginsel en andere beginselen uit de AVG gebeurt door de inzet van zogenaamde "verdedigingslinies". De staat van dat deel van de organisatie volgt hierna.

Allereerst heeft de universiteit op dit onderdeel weinig tot geen duidelijke stappen gezet. Verwerkingsdoelen worden veelal informeel[57] bepaald en de RUG kent nog onvoldoende uniformering op dit vlak. Dit resulteert in (decentrale) verwerkingen die naar hun aard gelijk zijn, maar in doelen uiteenlopen. Doelen liggen derhalve niet altijd in lijn met hetgeen wordt gecommuniceerd. De Algemene privacyverklaring Rijksuniversiteit Groningen ("privacyverklaring") omvat wel globaal de doelen van de verwerkingen bij de RUG. Effectieve controle op doelbinding[58] is desondanks nog niet mogelijk. In theorie zouden de vele duizenden individuele verwerkingen periodiek gecontroleerd moeten worden om iets zinnigs over de rechtmatigheid van de doelen te kunnen zeggen. Dit is simpelweg niet werkbaar.

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.[59]

Naast doelbinding is de borging van effectief intern toezicht gewenst. Dit geldt voor alle niveaus in de organisatie. Onder de paragraaf "Intern toezicht" wordt dit verder uiteengezet.

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 hebben voor de organisatie zelf.

[57] 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.
[58] Doelbinding houdt in dat persoonsgegevens niet nog voor andere (onverenigbare) doelen worden ingezet dan de doelen waarvoor ze initieel zijn verzameld.
[59] Binnen de RUG is het centrale privacyteam in samenwerking met de P&S-coördinatoren gestart met het uniformeren van de processen en verder specificeren van de doelen. Resultaten worden in 2021 verwacht.

Uniforme doelen na 2020

In het laatste kwartaal van 2020 is vanuit het centrale privacyteam een start gemaakt met het uniform beschrijven van verwerkingen en doelen. Hierbij zijn de P&S-coördinatoren betrokken om in gezamenlijkheid tot duidelijk omschreven, werkbare en veilige verwerkingen te komen. Die samenwerking vormt een belangrijke stap om van de papieren realiteit te komen tot een zorgvuldige praktijk.

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. Meer over het intern toezicht volgt hierna.

Intern toezicht

Binnen de universiteit is het interne toezicht op privacymanagement verdeeld in verschillende verdedigingslinies. Bij reguliere werkzaamheden zijn de uitvoerende medewerkers diegene die proberen op een zorgvuldige manier met persoonsgegevens om te gaan, kortom, zij zijn de eerste lijn.

In de tweede lijn bevinden zich de privacy- en securitycoördinatoren (P&S-coördinatoren), faculteitsbesturen en directies, maar ook het centrale privacyteam en de ethische commissies. Onduidelijk is nog welke rol de datastewards en het GDCC hebben bij het interne toezicht. Zie ook hoofdstuk 3 Privacybeleid en inbedding in de organisatie.

Leg vast welke rol datastewards en het GDCC krijgen binnen het interne toezicht.

In de derde lijn bevindt zich de IT-auditor en de functionaris gegevensbescherming (“FG”). In de vierde lijn bevindt zich de Raad van Toezicht (“RvT”) en de Universiteitsraad. Ook de Autoriteit Persoonsgegevens (“AP”) bevindt zich in de vierde lijn.

De entiteiten in de vierde lijn zullen voor een goede invulling van hun rol gebruikmaken van de observaties en adviezen die de IT-auditor en FG afgeven. Het jaarverslag van de FG, de Jaarrapportage bescherming persoonsgegevens, bevat de kern.

Het jaarverslag 2019 heeft in 2020 niet geleid tot het planmatig beperken van de omschreven risico’s op centraal niveau.

2020 was ook het eerste jaar waarin het CvB noch de RvT het jaarverslag met de FG hebben besproken. Ondanks meerdere verzoeken van de FG heeft een gesprek tussen de RvT en de

FG dit jaar niet plaatsgevonden. Desgevraagd heeft de AP de FG geadviseerd over deze afwijkende situatie.[60]

Los van het jaarverslag heeft het CvB wel een belangrijke stap gezet om in lijn met adviezen van de CISO en FG meer te sturen op risicobeperking. De stuurgroep Privacy & Security is in het leven geroepen om effectiever organisatiebrede risico's te mitigeren. De stuurgroep bestaat uit vertegenwoordiging van het CvB, de faculteiten, het CIT en ABJZ. Daarnaast nemen de CISO en de FG zitting in de stuurgroep als adviserende leden.

De FG tijdig betrekken en informeren

De coronacrisis is al meer dan een jaar de nieuwe realiteit. Daarmee krijgen onderwijs, onderzoek en bedrijfsvoering andere vormen. Voor de privacy van betrokkenen (studenten, medewerkers en onderzoeksdeelnemers) hoeft dit geen probleem te zijn.

Het op niveau houden van de volwassenheid van de privacymanagementorganisatie valt of staat gedurende de crisis met het toepassen van privacy by design. Kortom: het toepassen van de beginselen uit de AVG binnen (nieuwe) processen en systemen. Daarnaast is het betrekken van de FG cruciaal bij besluitvorming die de privacy raakt.[61]

In het afgelopen jaar is de FG op een aantal grote thema's niet tijdig betrokken en/of geïnformeerd. Hieronder vallen "online proctoring" en "registratie coronaklachten".[62]

Betrokkenheid van de FG in een later stadium mondt vaak uit in een vorm van toezicht en een negatief sentiment: "iets mag niet van de AVG/FG".[63] Indien de FG tijdig betrokken wordt, kan zijn advies meegenomen worden en processen privacyvriendelijk(er) worden ingericht.

De volwassenheid van de universiteit krijgt een impuls als deze manier van werken de standaard wordt. Dat komt tegemoet aan de veelvuldig uitgesproken wens van het CvB om te groeien naar een hoger volwassenheidsniveau.

Betrek de FG tijdig bij alle aangelegenheden die de verwerking van persoonsgegevens raken, vooral in crisistijd. Borg deze verplichting in het proces voorafgaand aan de besluitvorming. Het opnemen van de FG in het bestuurs- en beheersreglement draagt daaraan bij en wordt ook geadviseerd.[64]

[60] "[..] De leden van de RvT bewijzen zichzelf geen dienst door niet op de hoogte te zijn van de risico's op het gebied van privacy en gegevensbescherming. De FG is er juist om de verantwoordelijken van inzicht en advies te voorzien zodat zij acties kunnen laten nemen om AVG compliant te zijn. [..] Wanneer de RvT dan bijvoorbeeld aangeeft dat u gegevensbescherming beter kunt bespreken op een lager niveau dan kunt u in ieder geval gedocumenteerd laten zien dat u de poging heeft ondernomen de RvT in kennis te stellen.[..]"
[61] Zie artikel 38 lid 1 AVG: De verwerkingsverantwoordelijke en de verwerker zorgen ervoor dat de functionaris voor gegevensbescherming naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.
[62] De FG haakt uiteindelijk op eigen initiatief aan, maar is niet betrokken bij het ontwerp van een verwerking.
[63] Op decentraal niveau wordt dit ook ervaren door de privacy- en securitycoördinatoren ten aanzien van hun werk.
[64] Handreiking voor het versterken van de privacygovernance bij HO-instellingen, Platform Integrale Veiligheid Hoger Onderwijs / KPMG, februari 2021, conceptversie.

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 geeft de RUG inzage in de manier waarop zij omgaat met persoonsgegevens. Meerdere onderdelen uit dit jaarrapport komen dan ook samen in het register.

In 2019 is een grote (technische) stap gezet door de registertool “Privacy Perfect” in te richten. Systemen op zichzelf zorgen niet voor het actuele en volledige overzicht waarna de RUG streeft. Voor dat complete overzicht is de medewerking van elke faculteit en dienst nodig. Daarbij is het voor de domeinen onderwijs en bedrijfsvoering eenvoudiger te bewerkstelligen, omdat de processen (lees: verwerkingen) minder frequent wijzigen. Daarentegen is het domein onderzoek dynamischer. Onderzoeken zijn zelden identiek aan elkaar. Wel is er overlap in de gebruikte methodieken en vallen zogenaamde scenario’s te onderscheiden.

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.[65]

Privacy Perfect maakt een strictere controle aan de poort mogelijk. Het uitgangspunt is: P&S-coördinatoren beschrijven gezamenlijk met de leden van het privacyteam (ABJZ) de verwerkingen. De beschreven verwerkingen dienen daarna wel het uitgangspunt te zijn voor de centrale en decentrale uitvoering. Op die manier worden technische en organisatorische maatregelen, maar ook doelen[66] op een organisatiebrede wijze bepaald.

[65] Deze verplichting is te vinden in art. 30 lid 4 AVG.
[66] Zie hiervoor ook hoofdstuk 5 over doelbinding bij de RUG.

De “oude” registertool, de RDMP-tool[67], kent circa 1.800 beschreven verwerkingen. Een deel van die verwerkingen is besproken en herschreven om geüniformeerd in Privacy Perfect geplaatst te worden. Privacy Perfect telt op het moment van schrijven 60 verwerkingen.

Voor de eerste keer beschrijven van de verwerkingen, inclusief de passende technische en organisatorische maatregelen, is een tijdrovende klus. Dit levert uiteindelijk wel een landschap van verwerkingen op die in lijn zijn gebracht met de beginselen uit de AVG.

Bij die beginselen kan gedacht worden aan transparantie richting de betrokkene (duidelijk maken wat we met hun persoonsgegevens doen), dataminimalisatie (niet meer persoonsgegevens verwerken dan noodzakelijk), opslagbeperking (persoonsgegevens niet langer bewaren dan noodzakelijk) en vertrouwelijkheid (hoe beschermen we persoonsgegevens).

Belangrijk is om op decentraal niveau te komen tot een zorgvuldige verwerking van persoonsgegevens.[68] 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

Onderzoeken met persoonsgegevens worden in beginsel niet opgenomen in Privacy Perfect. Of en waar het overzicht van deze onderzoeken te vinden is, is afhankelijk van de faculteit. Bij de Faculteit GMW (“GMW”) is de Research Portal[69] ontwikkeld. Hierin wordt de onderzoeker meegenomen langs de fases van een onderzoek. Ook de afhandeling van de ethische toetsing vindt plaats in de Research Portal.

De Research Portal kan helpen bij het tonen van een actueel overzicht van onderzoeken met persoonsgegevens. Bij GMW zijn in 2019 de eerste onderzoeken hierin opgenomen. In 2021 worden alle onderzoeken van GMW hierin opgenomen. Niet alle faculteiten werken echter met de Research Portal, maar bijvoorbeeld wel met het alternatief: de RDMP-tool. Ook zijn er faculteiten die überhaupt de verwerkingen niet in kaart brengen of registreren.

Faculteiten hebben geen volledig overzicht van de onderzoeken (met persoonsgegevens). 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.

Om verwerkingen binnen onderzoek in beeld te krijgen, is de Research Portal een bruikbaar middel. Het gebruikt voorkomt extra administratieve handelingen voor onderzoekers omdat het processen combineert en dus meerdere doelen bereikt.

---

[67] De Research Datamanagement Plan-tool is ontwikkeld om datamanagementplannen voor onderzoek te maken en is te vinden op www.rug.nl/research/research-data-management/tools-services/rdmp/rdmp-web-tool.
[68] Bij een zorgvuldige verwerking worden beginselen als transparantie, dataminimalisatie, opslagbeperking, integriteit en vertrouwelijkheid meegenomen.
[69] De Research Portal wordt ook wel de Virtual Research Environment genoemd, maar zijn (nog) niet hetzelfde.

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.[70]

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

Verder bevat de RDMP-tool bij een aantal faculteiten nog geen aanwijzingen voor de te hanteren bewaartermijnen en omschrijving van de technische en organisatorische beveiligingsmaatregelen. De geregistreerde verwerkingen missen die details dus ook.

Het advies is om op decentraal niveau gestandaardiseerde processen[71] vast te stellen die in beginsel moeten worden gevolgd binnen de desbetreffende faculteit. Bij de vormgeving van deze processen worden minimale beveiligingsmaatregelen en indien mogelijk 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 het gros van de gezamenlijke verwerkingen binnen de domeinen bedrijfsvoering en onderwijs in kaart te brengen. De vorderingen stagneren momenteel omdat er bij de RUG geen verantwoordelijke is aangewezen voor de afstemming met het UMCG en verdere invulling van het register.

De RUG dient een verantwoordelijke aan te wijzen die bewaakt dat de doelen uit de Raamovereenkomst worden nageleefd.[72] Hieronder valt tevens de beschrijving van de verwerkingen in onderzoek en de (gedeelde) verantwoordelijkheden daarbij.

[70] Zie hiervoor ook de opmerkingen in hoofdstuk 4 onder “Onderzoek(ers)”.
[71] De gestandaardiseerde processen worden gebaseerd op de thans geregistreerde verwerkingen. Deze processen worden ook wel “onderzoekscenario’s” genoemd en beperken de academische vrijheid niet of minimaal.
[72] Dit sluit aan bij de bevindingen over het beheer op de verwerkersovereenkomsten in hoofdstuk 11.

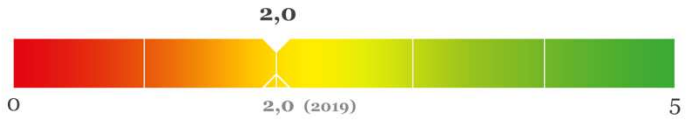
7. Kwaliteitsmanagement

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 het kunnen rectificeren, aanvullen, verwijderen en beperken van de verwerking van persoonsgegevens valt hieronder. Dit laatste is binnen de RUG behoorlijk geregeld. Het bewaken van de juistheid van persoonsgegevens vraagt meer aandacht.

Het niveau van kwaliteitsmanagement over de hele linie is ongewijzigd gebleven. Wil de RUG verder groeien, dan is meer aandacht vereist voor de bewaking van de nauwkeurigheid van persoonsgegevens. Dit geldt voor processen in grote systemen als AFAS[73], maar minstens zozeer voor de daaraan verbonden processen en systemen.

Naast het borgen van de juistheid gaat de RUG op een zorgvuldige wijze om met de verzoeken tot wijziging of verbetering van persoonsgegevens. Een dergelijk verzoek van een betrokkene is gebaseerd op het recht op rectificatie. De afhandeling van deze verzoeken gebeurt organisatiebreed op eenzelfde wijze en wordt uitgevoerd door het privacyteam en bewaakt door de FG. Hoe betrokkenen zich kunnen beroepen op deze en andere rechten zijn helder beschreven in de compacte privacyverklaring van de RUG.[74]

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 gegevens continu gesynchroniseerd tussen het systeem Studielink en de grotere onderwijssystemen binnen de RUG.[75] Wanneer studenten zich aanmelden via Studielink,

[73] Met AFAS wordt er gedoeld op AFAS Insite.
[74] Zie Bijlage 1. Compact model privacyverklaring RUG voor een voorbeeld.
[75] Studielink synchroniseert met Progress.NET. Progress.NET heeft een aantal koppelingen met andere systemen.

wordt 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 SIA om middels intelligente scanners de echtheid van identiteitsbewijzen te verifiëren. Middels deze scanners zijn accuratere controles uit te voeren en levert dit de RUG een tijdsbesparing op. Ondanks een lange onderbreking is het project eind 2020 weer gecontinueerd en wordt naar verwachting in Q2 2021 de nieuwe verificatiemethodiek ingezet binnen het aanmeldproces.

Parallel in Excel

Naast de (grote) onderwijssystemen worden binnen de RUG nog steeds studentgegevens verwerkt in Excel-bestanden en soortgelijke documenten.[76]

De studentgegevens binnen dergelijke documenten zijn per definitie niet actueel en mogelijk incorrect door het ontbreken van synchronisatiemogelijkheden.

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

Wil een student zijn naam, nationaliteit, verblijfplaats, huwelijkse staat en e-mailadres wijzigen dan kan hij/zij terecht bij de Basisregistratie Personen ("BRP") van de overheid en in het systeem Studielink. Overige gegevens kunnen worden gewijzigd bij de faculteit of SIA.

Persoonsgegevens van medewerkers

Het jaar 2020 stond in het teken van een turbulente start van AFAS. Naast de financiële processen, werd een groot deel van de HR-processen van PeopleSoft overgeheveld naar AFAS.

Bij de migratie van de data is veel aandacht geweest voor de juistheid van die data in alle stadia. Een gespecialiseerd bedrijf heeft hierop toegezien en de RUG begeleid.

Het aantal onjuistheden binnen de personeelsdossiers is hiermee tot een minimum beperkt.

[76] Een dergelijk beeld werd in 2018 en 2019 reeds geschetst door eigenaren en beheerders van de systemen, maar ook in 2020 bevestigd door de decentrale studentenadministraties.

Naast de migratie is borging van de juistheid van persoonsgegevens in AFAS nog steeds belangrijk. Op dit moment krijgen medewerkers niet bij elke wijziging van hun persoonsgegevens een melding. In het geval van onjuiste wijzigingen wordt de medewerker niet in staat gesteld om gegevens (direct) te rectificeren. Ook toont de wijzigingsgeschiedenis veel van de wijzigingen in AFAS niet.[77]

Na AFAS vormt Picobello een belangrijk knooppunt van persoonsgegevens. Hierin zijn ook de persoonsgegevens van medewerkers opgenomen. Naast een aantal systemen met een actieve gegevensuitwisseling bestaan er systemen die niet actief gevoed worden. Middels geëxporteerde lijsten met persoonsgegevens worden (decentrale) processen gevoed.

De RUG kent ook een aantal “niet-gekoppelde” systemen zoals 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.

Kwaliteitsmanagement is echter niet (geheel) afhankelijk van technische koppelingen/maatregelen. Organisatorische borging is minstens 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 onderzoeksdeelnemers

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 het kwaliteitsmanagement binnen specifieke onderzoeksprojecten, anders dan op het verwerkingsniveau door de onderzoeker, vindt organisatiebreed noch structureel plaats.[78]

In hoofdstuk 3 is reeds het wisselende kennisniveau bij onderzoekers ten aanzien van privacy en security aangestipt. Hetzelfde geldt voor de ethische commissies en de facultaire onderzoeksondersteuning. Het kennisniveau van het kwaliteitsmanagement van persoonsgegevens is daarom wisselend.

De motivatie om persoonsgegevens correct en actueel te houden komt niet per se voort uit de drang naar compliance met de privacywetgeving. Onderzoekers streven namelijk al naar een optimale kwaliteit van “hun” data om zuivere en valideerbare onderzoeksresultaten te kunnen publiceren. Dit komt het kwaliteitsmanagement van persoonsgegevens echter wel ten goede.

[77] Voorbeeld van een dergelijke wijziging betreft een aanpassing in de adresgegevens van een medewerker.
[78] Bewaking vindt incidenteel plaats door de ethische commissie, de facultaire onderzoeksondersteuning, het Research Data Office en/of de FG.

Op operationeel niveau wordt de borging van kwaliteitsmanagement door de onderzoeker beschreven in het datamanagement plan van het onderzoeksvoorstel. Binnen dit plan wordt de bescherming van persoonsgegevens behandeld in de vorm van uitgangspunten als transparantie en verifieerbaarheid van onderzoek en hergebruik van onderzoeksgegevens.[79]

Los van WMO-plichtig onderzoek (in samenwerking met het UMCG) kent de RUG geen specifieke richtlijnen ten behoeve van kwaliteitsmanagement van persoonsgegevens in onderzoek. Dit aspect wordt behandeld in de Gedragscode WI en de Gedragscode voor gebruik persoonsgegevens in wetenschappelijk onderzoek[80] ("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".[81] Binnen de handleiding wordt het aspect datakwaliteit kort behandeld en toegelicht.

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

[79] M. van Berchum, & M.J. Grootveld, 'Het beheren van onderzoeksdata', *Handboek Informatiewetenschap*, IV B 475, Vakmedianet, 2016, p. 2-3.
[80] De gedragscode stamt uit 2005 en is verouderd. Er wordt vanuit de VSNU gewerkt aan een nieuwe gedragscode.
[81] Ook de e-learningmodule Privacy in research: "asking the right questions" is hiervoor geschikt.

8. Bewaren van persoonsgegevens

De AVG geeft voor de verwerking van persoonsgegevens geen bewaartermijnen, maar kent 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 serieuze stappen gezet om bewaartermijnen beter na te leven.

Op basis van de Archiefwet zijn overheidsorganen verplicht een selectielijst te hebben. Afgelopen jaar is de zogenaamde Selectielijst voor universiteiten en UMC's ("Selectielijst") vastgesteld.[82] De Selectielijst vervangt het vorige Basisselectiedocument en biedt handvatten voor bewaartermijnen in onderwijs, bedrijfsvoering en onderzoek. Daarnaast heeft de RUG de bewaartermijnen uit de Selectielijst opgenomen in een aantal bredere richtlijnen voor het onderwijs. Deze richtlijnen zijn in de basis met de privacy- en securitycoördinatoren opgesteld. Dit leidt tot een beter toepasbare richtlijn.

Om verder te groeien op dit onderdeel is effectieve implementatie nodig van de richtlijnen en daarmee de Selectielijst. Binnen alle domeinen zijn stappen gezet. Het helpt daarbij dat de afdeling Documentaire Informatievoorziening ("DIV") ook bezig is met een inhaalslag ten aanzien van digitaal werken en archiveren. De uitgangspunten van de AVG en de Archiefwet- en regelgeving komen grotendeels overeen: bewaren van gegevens en documenten zolang noodzakelijk en het hanteren van een omgeving die passend beschermd is.

Veel archief (met bijbehorende persoonsgegevens) bevindt zich nog op netwerkschijven, de Google Drive, in e-mailboxen en in applicaties die niet zijn aangesloten op het digitale archief (Corsa). Het heeft tijd nodig om de archivering en de bijbehorende procedures en processen zorgvuldig en zoveel mogelijk geautomatiseerd in te richten.[83]

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.

[82] De Selectielijst Universiteiten en Universitair Medische Centra 2020 is vastgesteld op 31 januari 2020.
[83] Memo voor de Privacy- en Securitycoördinatoren "Instructies bewaartermijnen en vernietigingsplichten", Algemeen Bestuurlijke en Juridische Zaken, Rijksuniversiteit Groningen, 22 februari 2021.

E-mail kent geen bewaartermijnen

Het medium e-mail maakt het naleven van bewaar- en vernietigtermijnen erg lastig. Bewaren is in veel gevallen eenvoudiger dan het (selectief en) tijdig verwijderen van gegevens. E-mailboxen van medewerkers met e-mail van 20 jaar terug is geen uitzondering.

De e-mail is in veel gevallen het collectief archief van de RUG waarbij de RUG dus persoonsgegevens verwerkt van (tien)duizenden mensen. Persoonsgegevens worden veelal langer verwerkt dan noodzakelijk. Daarmee voldoet de RUG niet aan de opslagbeperking en andere beginselen.[84] Dit geldt ook voor het beheer van stukken in het kader van de Archiefwet zolang stukken in de e-mail blijven staan.

Naast de e-mail is de omgang met bewaartermijnen binnen de drie grote categorieën van betrokkenen (studenten, medewerkers en onderzoeksdeelnemers) 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 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 succesvol uitrollen van Project DSD binnen de gehele RUG.

Naar aanleiding van het Project DSD zijn de werkprocessen van examencommissies al op een uniforme wijze uit te voeren. Dit betekent ook dat de toegankelijkheid, vertrouwelijkheid en bewaartermijnen van de persoonsgegevens gewaarborgd worden.

Veel persoonsgegevens zijn ondergebracht in systemen die niet archiefwaardig zijn. Denk hierbij aan Progress.NET, OAS en Stuf!. Deze systemen bevatten een veelheid aan persoonsgegevens die reeds vernietigd hadden moeten worden.

Op het moment van schrijven is een projectvoorstel in de maak voor het integreren van het archief met de systemen bij de SIA. Hiermee wordt ook een constante verbinding tussen het archief en Progress.NET gecreëerd. De gebruiker kan dus in Progress.NET blijven werken, maar het RUG vernietigingsprotocol wordt wel nageleefd.

Persoonsgegevens medewerkers

Met de komst van AFAS werd de mogelijkheid geboden om persoonsgegevens van personeel te verwijderen bij het bereiken van het einde van een bewaartermijn. AFAS voldoet echter (nog) niet aan de wettelijk gestelde eisen om in te kunnen archiveren (en vernietigen). Personeelsdossiers zijn daarom in het archief (Corsa) geplaatst waar bewaar- en vernietigingstermijnen kunnen worden gehandhaafd. Periodiek worden die dossiers aangevuld vanuit AFAS. Vanuit Corsa wordt middels een signaal aan de functioneel beheerders van

[84] Hetzelfde risico geldt ook voor de persoonsgegevens binnen de Business Intelligence Portal.

AFAS aangemerkt welke gegevens op hun beurt in AFAS vernietigd kunnen worden. Dit levert een redundante opslag van gegevens op.

Door de zogenaamde 'best practices' binnen AFAS tegen het licht van de Selectielijst te houden kan de RUG de bewaartermijnen naleven. Het koppelen van het archief met AFAS biedt hierbij het nodige houvast.

Persoonsgegevens onderzoeksdeelnemers

Binnen het onderzoeksveld worden de bewaartermijnen in beginsel overgelaten aan de onderzoekdisciplines. De Selectielijst 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 waarde) van de data te worden getoetst aan de belangen voor maatschappelijke bewaring zoals 'open science'. [..]"

Gemiddeld genomen wordt 10 jaar[85] 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 RUG 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[86] 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 disciplinespecifieke richtlijnen vorm krijgen. Bij het opstellen van richtlijnen is de inbreng van onderzoekers en de ethische commissies cruciaal.

[85] De Faculteit Gedrags- en Maatschappijwetenschappen hanteert een minimale bewaartermijn van 10 jaar voor ruwe data, maar nuanceert voor wat betreft persoonsgegevens. Die bewaartermijn is afhankelijk van verificatie- en onderzoeksdoelen, maar ook van de getroffen (beveiligings)maatregelen zoals pseudonimisering.
[86] 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. De verwevenheid wordt duidelijk wanneer we kijken naar de incidenten bij de Universiteit Maastricht, NWO en de Universiteit van Amsterdam. Een goede borging van de privacy vraagt om passende technische en organisatorische maatregelen. Die organisatorische kant is net zozeer een uitdaging als de technische. Hoe gaat de RUG in tijden van crisis en incidenten om met de beveiliging?

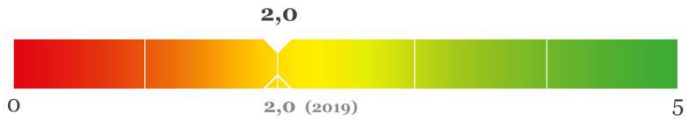
Allereerst, de AVG schrijft geen specifieke (technische) beveiligingsmaatregelen voor. Zij vraagt de RUG als verantwoordelijke om maatregelen te nemen die passen bij de stand van de techniek, uitvoeringskosten, omvang en context van de verwerkingen en hun doelen.

De belangrijkste stappen om de beveiliging van persoonsgegevens binnen de RUG te vergroten zijn in het voorgaande Jaarrapport gedeeld en veelal ongewijzigd gebleven. Sinds dat Jaarrapport heeft de CISO wel een beveiligingsplan[87] opgesteld en beschreven welke aspecten prioriteit dienen te krijgen. De voortgang wordt elk kwartaal met het CvB besproken.

Opvallend is dat veel (technische) maatregelen middels een project bij het CIT worden geïnitieerd. De doorstroom van die projecten gaat moeizaam; dit kent meerdere redenen.[88] Daarnaast zijn veel technische maatregelen het resultaat van beleid en richtlijnen. Een “tool” of “functionaliteit” an sich is echter het halve werk. Hoe die in te zetten, door wie en de uiteindelijke werking is minstens zo belangrijk.

De RUG heeft stappen gezet op het terrein van beveiliging. De stappen hebben niet geleid tot verhoging in de volwassenheid. Daarvoor is organisatiebreed een periodieke analyse van beveiligingsrisico’s nodig en een meer geïntegreerd beveiligingsplan.

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.

[87] Roadmap informatiebeveiliging 2020-2021.
[88] Hierbij zijn vertrek van expertise, tekort aan personeel in het algemeen en schuring tussen teams de belangrijkste.

Bij het vaststellen van de externe (digitale) dreigingen en daarmee de risico's, is gekeken naar het Cybersecuritybeeld Nederland 2020 van de NCSC en het dreigingsbeeld van SURF.[89] Een deel van de risico's komt in dit hoofdstuk aan bod onder "**Fout! Verwijzingsbron niet gevonden.**".

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

De beslissingsbevoegdheid omtrent het minimale beveiligingsniveau ligt momenteel veelal op decentraal niveau en dat is niet wenselijk. Zoals we bij de eerder benoemde incidenten 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[90] 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[91] 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.

Een belangrijke wijziging in de governance is het aanwijzen van een CISO. De CISO legt verantwoording af aan het CvB en nu nog aan de directie van het CIT. Het afleggen van verantwoording aan de directie van het CIT is een weeffout. CIT is de interne IT-leverancier van de RUG.[92] Beveiliging van informatie(technologie) is niet haar primaire taak.

[89] Het dreigingsbeeld van de NCTV en NCSC (Nationaal Cyber Security Centrum): https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2020/juni/29/csbn-2020/CSBN+2020.pdf en SURF: https://www.surf.nl/files/2021-02/surf-cyberdreigingsbeeld-2020-2021.pdf.
[90] Binnen de RUG is de basisbeveiliging vastgelegd in de RUG Baseline.
[91] 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.
[92] 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.

Naast de governance achter de informatiebeveiliging, zijn er 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

Binnen de bedrijfsvoering vinden de alledaagse verwerkingen van persoonsgegevens plaats. Hier is winst te behalen met betrekking tot beveiliging. Hieronder worden risico's van betekenis benoemd en oplossingen voorgesteld; het betreft echter geen limitatieve lijst.

Autorisaties in AFAS

Met de ingebruikname van AFAS lopen veel van de financiële en HR-processen in AFAS. Met name de HR-processen bevatten veel (gevoelige) persoonsgegevens van personeel. Het is daarom belangrijk om de vertrouwelijkheid van die gegevens goed in te regelen. De structuur en invulling van autorisaties is daarbij essentieel. Met andere woorden: wie geef je toegang tot welke (persoons)gegevens. Dit is binnen de RUG nog niet goed ingeregeld.[93]

De RUG kende meerdere datalekken vanwege verkeerd ingeregelde autorisaties binnen AFAS. Dergelijke datalekken doen zich nog steeds voor en raken medewerkers.

Uit de gesprekken met (HR-)medewerkers blijkt dat er onvoldoende is gedaan met de input van HR bij het inrichten van AFAS en meer specifiek de autorisaties. Het inregelen van financiële processen lijkt leidend in alle fasen van de introductie van AFAS. Dit uit zich nu ook door de verantwoordelijkheid voor de sturende én uitvoerende processen bij het FSSC neer te leggen. Het gevolg is ook dat zogenaamde "request for change" in AFAS niet beoordeeld worden op (privacy)risico's en privacy by design niet wordt meegenomen.

Binnen AFAS dient met een multi-disciplinair team gekeken te worden naar het verbeteren/inrichten van autorisaties. HR dient het eigenaarschap van de inrichting van processen in AFAS meer naar zich toe te trekken. Het inrichten van AFAS is vooral géén technische of enkel financiële aangelegenheid.

Met de recente koppeling van Salure aan AFAS worden eventuele gebreken in de autorisaties ook overgenomen in Salure. Dit is een extra reden om de autorisaties correct in te richten.

Onbeveiligde verwerking van (bijzondere) persoonsgegevens

E-mail is naast de Y-schijf en Google Drive nog steeds dé manier om documenten met (bijzondere) persoonsgegevens tussen A en B uit te wisselen. Binnen de RUG wordt het gros

[93] In de Jaarrapportage van 2019 is aangegeven dat de implementatie van AFAS veel processen kan verbeteren, ook in de zin van bescherming van persoonsgegevens, mits de autorisaties op orde zijn. Dit bleek in de maand voorafgaand aan de lancering van AFAS nog niet in orde. AFAS startte met meer dan 670 praktisch onbeheersbare functies (lees: rollen). Dat zijn er begin 2021 iets meer dan 214. Een gedeelte van de rollen heeft meer rechten gekregen dan strikt noodzakelijk; dat vereenvoudigde het indikken van de groep van functies.

van de e-mails niet versleuteld. Dit betekent dat kwaadwillenden die e-mail onderscheppen, deze ook kunnen lezen (en aanpassen).

In 2020 wordt nog geen gebruik gemaakt van versleutelde e-mail. 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.[94]

Google Workspace for Education biedt (kosteloos) versleuteling van het interne e-mailverkeer aan. Dit is een eerste stap. Daarnaast zal de RUG moeten kijken naar alternatieven voor e-mail, zoals Unishare.

Bij het aanbieden van veiligere alternatieven, zoals Unishare, is aandacht voor gebruiksgemak en richtlijnen rondom de veilige verzending van (bijzondere) persoonsgegeven bepalend voor de acceptatie door collega's en studenten.

Verder vormt het gebruik van persoonlijke e-mailadressen (@gmail.com, @live.com, @hotmail.com) om met collega's, studenten en onderzoeksdeelnemers te e-mailen een blijvend risico binnen de RUG. In veel gevallen is het gebruik in deze context te kwalificeren als een inbreuk in verband met persoonsgegevens (lees: een datalek).

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, waaronder marketing en het informeren van inlichtingendiensten.

Communicatie over het ongewenste gebruik via de centrale kanalen is aan te raden. Bied eventueel een alternatief aan indien het eigen @rug.nl-e-mailadres niet voldoet voor de specifieke doelen. Dit advies geldt ook voor de leden van het College van Bestuur zelf.

BYOD

Gedurende de coronacrisis wordt het meeste werk uitgevoerd op apparaten die niet door de RUG worden beheerd. Deze persoonlijke apparaten, ook wel "Bring your own device" (BYOD), vergroten de flexibiliteit en het gebruiksgemak. De vloot aan onbeheerde apparaten vormt voor de RUG echter wel een risico. (Persoons)gegevens blijven niet binnen beheerde IT-infrastructuur van de RUG.

Veel van deze apparaten zijn onvoldoende beveiligd. 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.[95]

---

[94] De Studenten Informatie & Administratie start Q2 2021 met een veiligere manier van controleren en verder verwerken van identiteitskaarten en paspoorten zonder (onbeveiligde) e-mail. De applicatie Verifai wordt hierbij gehanteerd.

[95] 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.

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

Registratie uitgegeven apparaten

In het verlengde van BYOD ligt het uitlenen van apparaten. Met de coronacrisis is dit nog meer van belang geworden. De RUG vertrouwt laptops en tablets toe aan haar medewerkers. De uitgeleende apparaten worden geregistreerd in Planon of fysiek gedocumenteerd bij de CIT Servicedesk.

In tegenstelling tot de uitgave gebeurt de inname van de apparaten niet gestructureerd. Niet alle apparaten worden ingeleverd. Het is derhalve niet mogelijk om de Baseline op dit moment 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. Hiermee wordt voorkomen dat vertrouwelijke gegevens op straat komen te liggen.

Met het gebruik van Planon en AFAS is een organisatiebreed proces in te richten en is de teruggave van apparaten te borgen. Naast de systemen is het beleid en werkwijze reeds door de demand managers, facility managers en HR ontwikkeld.[96]

Naast de bescherming van persoonsgegevens wordt fraude en/of verduistering ook beperkt.

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.

Reeds in 2018 is 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. Eind 2020 is het project pas weer opgepakt met een eerste deadline in Q2 2021 voor de versleuteling van alle nieuwe apparaten. De oudere apparaten worden daarna opgepakt.

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.

[96] A.J. Gankema e.a., "Registratie verstrekking RUG-faciliteiten aan medewerkers", Rijksuniversiteit Groningen, 22 november 2016.

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.

Implementeren van MFA

Het laatste punt van aandacht binnen het domein bedrijfsvoering ziet op de toepassing van meerfactorauthenticatie (MFA). MFA is een techniek waarbij de persoon of het systeem een combinatie van minimaal twee verschillende typen authenticatiefactoren moet gebruiken om toegang te krijgen. Bijvoorbeeld een wachtwoord én een eenmalige code (token) per sms.[97]

De Autoriteit Persoonsgegevens heeft aangegeven dat veel datalekken naar aanleiding van hacking, malware of phishing-incidenten voorkomen hadden kunnen worden voorkomen.[98]

AUTORITEIT PERSOONSGEGEVENS

Gezien de reële dreiging van hacks[99] op onderwijsinstellingen in Nederland, doet de RUG er verstandig aan om op zeer korte termijn MFA te implementeren op alle systemen waar ook Single Sign-on is ingesteld. Daarnaast is awareness en training van personeel noodzakelijk om (spear)phishingmail te herkennen en te neutraliseren.

Beveiliging bij onderzoek met persoonsgegevens

Onderzoeken met persoonsgegevens zijn beperkt in kaart gebracht (zie hoofdstuk 6 Register). Wanneer 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.

Het CIT en RDO (vanaf 2021: GDCC) bieden technische en organisatorische ondersteuning aan onderzoekers om onderzoeksdata (veiliger) te kunnen verwerken. Het kunnen aansluiten

---

[97] Rapportage Datalekken 2020, Autoriteit Persoonsgegevens, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapportage_datalekken_2020.pdf, 1 maart 2021, pg. 1.
[98] Rapportage Datalekken 2020, Autoriteit Persoonsgegevens, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapportage_datalekken_2020.pdf, 1 maart 2021, pg. 7.
[99] In februari van 2021 waren de Universiteit van Amsterdam, Hogeschool van Amsterdam, Hogeschool InHolland en het NWO slachtoffer van een cyberaanval.

bij zogenaamde onderzoekscenario's bevordert de dienstverlening en helpt de onderzoeker helder te krijgen welke maatregelen passend zijn voor het onderzoek. Onderzoekscenario's beschrijven bepaalde generieke handelingen binnen onderzoek of elementen uit een onderzoeksmethodiek. Een onderzoekscenario kan op haar beurt worden gekoppeld aan een set met (beveiligings)maatregelen.

Building blocks in onderzoek

Een set aan (beveiligings)maatregelen wordt binnen de RUG een building block genoemd. Om te komen tot de juiste building blocks voor (nieuw) onderzoek is het doen van een DPIA in beginsel het uitgangspunt.[100] Het uitvoeren van DPIA's op onderzoekscenario's maakt dat uiteindelijk niet voor elk individueel onderzoek meer een DPIA noodzakelijk is, zolang het onderzoek valt onder een van de uitgewerkte onderzoekscenario's.

Faculteiten dienen onderzoekscenario's te beschrijven waaraan zogenaamde sets van maatregelen ("building blocks") worden gekoppeld. De building blocks dienen door het GDCC toegankelijk te worden gepresenteerd voor de onderzoeker.

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

- pseudonimiseringsdienst;[101]
- anonimiseringsdienst;[102]
- versleutelen van opslagmedia;
- data veilig koppelen;
- database versleuteling;
- Virtual Reseach Workspace.

[100] Het richtsnoer "Starting with a DPIA methodology for human subject research" helpt de onderzoeker bij vragen over het DPIA.
[101] Bij pseudonimiseren worden gegevens die direct tot een persoon herleidbaar zijn uit een dataset verwijderd en separaat opgeslagen. Door te pseudonimiseren blijft de bruikbaarheid van de data hoog, terwijl de risico's voor betrokkenen sterk worden verminderd.
[102] 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

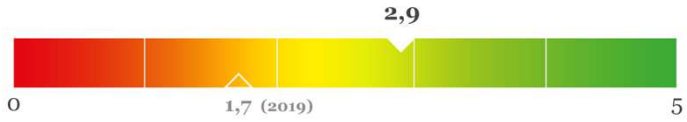
Transparantie is binnen het privacyrecht een groot goed en een van de beginselen. Van de RUG wordt verwacht dat zij transparant is over hetgeen zij doet met de persoonsgegevens van studenten, medewerkers en onderzoeksdeelnemers. Zij hebben op hun beurt een aantal rechten om (beperkte) controle te kunnen uitoefenen op die persoonsgegevens.[103] De manier waarop de RUG hiermee omgaat schept vertrouwen.

Op organisatieniveau kent de RUG een algemene privacyverklaring. Binnen deze privacyverklaring licht de RUG in grote lijnen toe hoe persoonsgegevens worden verwerkt en met welke doelen. Dergelijk inzicht is echter te abstract en niet specifiek genoeg.

Daarom stelt de RUG verklaringen op voor de betrokkenen binnen alle domeinen op verwerkingsniveau.[104] De verwerkingen met de hoogste risico's worden eerst beschreven. Hiervoor hanteert de RUG een standaard template van de privacyverklaring.[105] Deze compacte privacyverklaring verhoogt de leesbaarheid en verduidelijkt de verwerking met visuele elementen.[106]

Naast de "informatieplicht" heeft de RUG een organisatiebreed vastgestelde procedure voor het beantwoorden van de vragen (lees: rechten) van de betrokkenen. Dit proces loopt gestructureerd en is afgestemd op de categorie betrokkene.

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 resulteren in een boete of last onder dwangsom. Daarnaast kan een gebrek aan transparantie afbreuk doen aan het vertrouwen in en reputatie van een organisatie.

[103] De belangrijkste rechten zijn opgenomen in artt. 15 – 22 AVG.
[104] Bij het opmaken van nieuwe verwerkingen in het register wordt, indien noodzakelijk, een privacyverklaring opgesteld die de verwerking correct verwoordt. Middels een periodieke controle op de verwerkingen door de P&S-coördinatoren en het centrale privacyteam wordt de transparantie geborgd.
[105] Een voorbeeld is bijgevoegd als Bijlage 1. Compact model privacyverklaring RUG.
[106] Het compacte model is voorgelegd aan studenten en hun feedback is verwerkt in de huidige versie.

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.

Zoals in hoofdstuk 6 Register is beschreven zijn niet alle verwerkingen binnen de RUG in kaart gebracht. Dit maakt het beantwoorden van verzoeken van betrokkenen zeer arbeidsintensief en blijft het tijdig[107] beantwoorden een uitdaging.[108]

Aantallen inzageverzoeken en overige verzoeken

In 2020 heeft de RUG de volgende verzoeken op grond van de AVG ontvangen:

Recht op inzage:	**12**
Recht op rectificatie:	**0**
Recht op verwijdering[109,110]:	**28**
Recht op dataportabiliteit:	**0**

Van deze verzoeken heeft de RUG **11** inzageverzoeken en **9** 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 regels ten aanzien van de verwerking van persoonsgegevens. Er kan namelijk worden afgeweken van een aantal rechten van onderzoeksdeelnemers.[111] Dit kan betekenen dat de RUG besluit om de onderzoeksdeelnemer 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 komen.[112]

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

---

[107] 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.
[108] Ook is met de vervanging van een computersysteem bij Arbo, milieu en duurzaamheid (AMD) de koppeling naar oude dossiers van studentenpsychologen en daarmee (zeer vertrouwelijke) studentendossiers slecht vindbaar.
[109] In 19 van de 28 gevallen ging het om een geautomatiseerd verzoek tot verwijdering ("Data Removal Request").
[110] 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.
[111] Kaders voor wetenschappelijk onderzoek zijn terug te vinden in art. 89 lid 2 AVG jo. art. 44 UAVG.
[112] Deze beperking van het recht op verwijdering wordt gevonden in art. 17 lid 3 sub d AVG.

11. Verwerkersovereenkomsten en doorgifte

De RUG zet meer dan honderd organisaties in die in opdracht van haar persoonsgegevens verwerken. Deze verwerkers dienen een passend beschermingsniveau te hanteren. Dit wordt vastgelegd in een zogenaamde verwerkersovereenkomst.[113] Het hoge beschermingsniveau dient buiten Nederland en de EER[114] ook te worden gehandhaafd. Dat is met de uitspraak van de Europese rechter in 2020 moeilijker geworden.

Het verstrekken van persoonsgegevens aan derden wordt “doorgifte” genoemd. Doorgiftes vinden plaats aan verwerkers van de RUG, zoals AFAS, Blackboard en Google, maar ook aan andere universiteiten bij een gezamenlijk onderzoek. Dit wordt binnen de RUG vastgelegd in het verwerkingenregister en de Research Portal.

Doorgifte naar organisaties buiten de EER wordt met de uitspraak in 2020 ingewikkelder. Op 16 juli heeft de hoogste Europese rechter in de Schrems II-zaak (“Schrems II”)[115] het Privacy Shield ongeldig verklaard. Privacy Shield bestond uit een set van afspraken die het mogelijk maakte om persoonsgegevens legitiem tussen de EU en de VS uit te wisselen.

De uitspraak heeft gevolgen voor de RUG voor wat betreft de diensten en producten waarbij sprake is van verwerking van persoonsgegevens van medewerkers, studenten en derden met partijen buiten de EER.

De doorgiftes van persoonsgegevens aan verwerkers worden door de RUG vastgelegd in de standaard-verwerkersovereenkomst. Deze is gebaseerd op het landelijke model van SURF.[116] Als gevolg van Schrems II is meer aandacht vereist bij de doorgifte buiten de EER en dus ook bij het afsluiten van verwerkersovereenkomsten.

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.

[113] De verplichting om een verwerkersovereenkomst te sluiten met verwerkers wordt gevonden in art. 28 lid 3 AVG.
[114] Europese Economische Ruimte bestaat uit de EU-landen met daarbij Liechtenstein, Noorwegen en IJsland.
[115] HvJ EU 16 juli 2020, C-311/18, ECLI:EU:C:2020:559 (*Schrems II*).
[116] SURF is een coöperatie van universiteiten, hogescholen en mbo-instellingen die werken aan ICT-innovatie.

Beheer verwerkers- en samenwerkingsovereenkomsten

Op dit ogenblik heeft de RUG met circa 130 verwerkers een getekende overeenkomst. Daarnaast kent de RUG ook tientallen (wellicht honderden) partijen waarmee zij gezamenlijk optrekt bij de verwerking van persoonsgegevens. Ook wel Joint Controllers genoemd.

Voor het afsluiten van verwerkersovereenkomsten weten de P&S-coördinatoren de privacysectie van ABJZ goed te vinden. Naast ABJZ heeft het CIT ook extra personeel aangetrokken om sneller leveranciers te kunnen contracteren.[117] Zo kan het onderwijs door.

Om de verwerkersovereenkomsten efficiënt en effectief te beheren, worden de eisen die de RUG aan derden stelt geüniformeerd en zijn afspraken intern voor eenieder helder. Enkel in uitzonderlijke situaties wordt afgeweken van de standaard-verwerkersovereenkomst.

Dit geldt nog niet voor de overeenkomsten met andere “verantwoordelijken”. Dit zijn partijen als onderzoeksinstituten en partneruniversiteiten waarmee de RUG onderzoekssamenwerkingen respectievelijk joint degree programma’s opzet. Bepalingen over de bescherming van persoonsgegevens in deze overeenkomsten ontbreken of zijn veel te summier beschreven.

Naleving door verwerkers

Veel (verwerkers)overeenkomsten zijn gesloten. Adequaat beheer van het gewenste niveau van beveiligingsmaatregelen en het organisatiebreed monitoren van doorgifte buiten de EER is echter beperkt mogelijk. Bij de RUG ontbreekt een beheeromgeving voor (verwerkers)-overeenkomsten.

(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, doorgifte buiten de EER en de gestelde eisen omtrent de bescherming van persoonsgegevens.

Heeft de RUG eenmaal afspraken met haar verwerkers gemaakt, dan is zij als verantwoordelijke verplicht om de naleving daarvan te (laten) toetsen; oftewel te auditen.

Audits op de (maatregelen in de) verwerkersovereenkomst worden door de RUG nog zelden uitgevoerd. Het besluit tot auditen gebeurt momenteel informeel en is afhankelijk van de keuze van een (decentrale) eenheid. Deze handelwijze is ongewijzigd ten opzichte van die in het jaarrapport 2019 beschreven staat.

In 2020 is een IT-auditor aangesteld wiens werk voor een derde uit “privacymanagement” bestaat. De IT-auditor is de persoon bij uitstek om adequaat de overeengekomen maatregelen bij verwerkers te (laten) auditen.

Bepaal aan de hand van het risico van een verwerking of en wanneer een audit wordt uitgevoerd bij een verwerker. Plan de audits in overleg met de IT-auditor, CISO en FG.

[117] Een voorbeeld is de afdeling ESI binnen het CIT. ESI heeft te maken met een groot aantal applicaties waarvoor afspraken met leveranciers vereist zijn.

Onrechtmatige doorgifte van AFAS aan Google

Dat naleving ook voor de grote verwerkers niet vanzelfsprekend is, bewijst AFAS. In AFAS kan een medewerker zijn adres wijzigen. De pagina in kwestie bevat echter ook een zogenaamd iframe van Google Maps dat het adres van de medewerker plot op een kaart.

De programmatuur van AFAS zet zonder (contractuele) toestemming van de RUG en/of de medewerker persoonsgegevens (adresgegevens) door aan Google. Deze gegevens worden door Google verwerkt voor doeleinden vermeld in de “Google Privacy Policy” en omvatten commerciële doelen, zoals het tonen van advertenties.

De doorgifte is volgens de FG een onrechtmatige verwerking en kan gekwalificeerd worden als een datalek. De situatie is vanaf april meermalen aangekaart bij het BestPractice-team en bij de FG van AFAS.[118] De omstandigheden zijn echter niet gewijzigd.

Draag zorg voor een privacyvriendelijke manier om woon-werkverkeer te berekenen. Hierbij kan gekeken worden naar de implementatie van een open source kaart.

Doorgifte buiten de EER en Brexit

Het niveau van bescherming van persoonsgegevens dat 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 de voorwaarden uit de AVG wordt voldaan.

Als gevolg van Schrems II kan de RUG de doorgifte van persoonsgegevens aan de VS niet langer baseren op het Privacy Shield. Alternatieven zijn echter beperkt aanwezig. Het is voor de RUG daarom belangrijk om zo spoedig mogelijk te inventariseren welke afspraken zijn gemaakt met derden in de VS (en overige landen buiten de EER).

In lijn met de inventarisatie moet per verwerker worden gekeken of aanpassingen in de overeenkomst noodzakelijk zijn. Het beperken, wijzigen of stoppen met de doorgifte van persoonsgegevens kan dan een conclusie zijn.

Ook het Verenigd Koninkrijk (“VK”) vergt een soortgelijke handelwijze. Op 31 januari 2020 verliet het VK de Europese Unie. Tot 1 mei 2021 geldt hetzelfde regime van doorgifte van persoonsgegevens als voorheen. Daarna is de omgang met het VK afhankelijk van de gemaakte afspraken. Een zogenaamd adequaatheidsbesluit[119] valt te verwachten, maar staat niet vast.

[118] De FG van AFAS kwalificeert het volledige adres in deze situatie niet als persoonsgegevens. Ook is hij van mening dat AFAS geen (sub)verwerkersovereenkomst met Google hoeft af te sluiten. Dit strookt niet met hetgeen de AP hierover schrijft: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens en https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verwerkers?qa=verwerkersovereenkomst.

[119] Met een adequaatheidsbesluit stelt de Europese Commissie vast dat het beschermingsniveau van het Verenigd Koninkrijk passend is. In dat geval blijft vrij verkeer van persoonsgegevens, zoals voorheen, naar het VK mogelijk.

Zonder zo'n besluit wordt het VK een zogenaamd derde land en gelden de reguliere voorwaarden uit de AVG. Deze voorwaarden hanteert de RUG reeds bekend bij doorgiftes.

Strategie buitenlandse techbedrijven

In het verlengde van Schrems II en het DPIA op G Suite (zie hoofdstuk 4) vraagt de huidige verstandhouding met de (grote) buitenlandse techbedrijven een nieuwe handelwijze. De Rectores magnifici betoogden in 2019 al het volgende:

[..] Onderwijs is een publiek goed, het dient breed toegankelijk te blijven. De onafhankelijkheid mag niet in het geding komen, de rechten en vrijheden van studenten en medewerkers − zoals privacy en non-discriminatie − moet gewaarborgd zijn. En het publiek toezicht moet zijn gegarandeerd. Die waarden dienen voorop te staan, ook bij digitalisering en het gebruik van commerciële platformen. [..].[120]

Wil de RUG de rechten en vrijheden van studenten en medewerkers waarborgen, dan is het formuleren van een duidelijke strategie een eerste stap. Hoe gaan we als universiteit om met de doorgifte van persoonsgegevens en onder welke voorwaarden vindt er al dan niet doorgifte plaats naar specifieke landen/werelddelen.

Op het ogenblik wordt de discussie met name gevoerd vanuit een juridisch perspectief. Daarbij wordt gekeken naar de (privacy)wetgeving en hetgeen vanuit de gezamenlijke Europese toezichthouders wordt geadviseerd. Het vraagstuk wordt daarmee slechts eenzijdig belicht.

Doorgifte van onderzoeksgegevens

Binnen onderzoek is "open science" het devies en worden veelal de FAIR-principes gehanteerd. Om hergebruik van onderzoeksdata mogelijk te maken volgens het uitgangspunt "open, tenzij", is het belangrijk dat datasets zoveel mogelijk worden gepseudonimiseerd. Zo zijn gegevens in beginsel niet te herleiden tot onderzoeksdeelnemers.

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

Controle op de te publiceren datasets vindt binnen DataverseNL al wel plaats door het RDO.[121] Dit gebeurt in principe nog niet bij datasets in andere data repositories.

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 aanwezig te zijn. Ook is aan te raden om steekproefsgewijs de publicatie van datasets bij andere repositories te controleren. Hier kan het GDCC en/of de faculteit een belangrijke rol spelen.

---

[120] Digitalisering bedreigt onze universiteit, *De Volkskrant*, 23 december 2019.

[121] Aanbevelingen kunnen zijn: variabelen hercoderen, classificeren, verwijderen van bepaalde variabelen (mits dat wetenschappelijk verantwoord is) of het niet open maar restrictief opnemen van de dataset in de repository.

12. Datalekken

In 2020 was het aantal gemelde datalekken iets hoger dan in 2019. De processen binnen AFAS hadden een hoofdrol binnen het totale overzicht van incidenten. Door tekortkomingen in de autorisaties waren meer gegevens inzichtelijk dan strikt noodzakelijk. Los daarvan is de procedurele afhandeling van incidenten en datalekken binnen de RUG verbeterd en zijn stappen gezet om (toekomstige) incidenten te beperken. Er wordt meer geleerd van afgeronde incidenten.

In de privacywetgeving wordt niet gerept over “datalekken”, maar over “inbreuk in verband met persoonsgegevens.” Voor de leesbaarheid van deze rapportage wordt “datalekken” gehanteerd. Niet alle incidenten en datalekken worden nog gemeld door medewerkers en studenten. Zij hebben namelijk een sterk ingekleurd en te beperkt beeld van een datalek.[122] *De verloren USB-stick* is nog steeds hét standaardvoorbeeld, maar is niet illustratief voor het gemiddelde datalek bij de RUG.

Vergeleken met het voorgaande jaar worden datalekken met een zogenaamd laag-risicoprofiel niet langer direct bij het CvB gemeld, maar afgehandeld door het hoofd van ABJZ. Dit zorgt voor focus bij het CvB op datalekken met meer impact.

Naast de afhandeling van datalekken is het voorkomen van datalekken nu onderdeel van veel richtlijnen over thuiswerken, gebruik van online diensten en berichtenapps. Deze richten zich voornamelijk op bedrijfsvoering en onderwijs. Handvatten om incidenten binnen onderzoek te voorkomen zijn schaars of slechts informeel aanwezig. Dit is een groeikans voor de RUG op dit onderdeel.

Het volwassenheidsniveau op dit onderdeel binnen de RUG:

Algemene risico’s

Datalekken kunnen negatieve gevolgen hebben voor de levenssfeer van betrokkenen (medewerkers, studenten en onderzoeksdeelnemers). 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.

[122] Onder een datalek valt ook het per ongeluk, maar definitief verwijderen van persoonsgegevens, het ongeautoriseerd wijzigen van persoonsgegevens of de verwerking zonder gerechtvaardigde grondslag.

Naast de splitsing die is aangebracht in de afhandeling van incidenten met een laagrisicoprofiel en diegene met een middel-/hoogrisicoprofiel, is ook gestart met een terugkoppeling per kwartaal aan het CvB. Dit behelst de bespreking van het geheel aan incidenten en de controle op de uitvoering van de voorgestelde maatregelen.

In 2020 is op voordracht van de CISO 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.

Inventarisatie datalekken

In heel 2020 zijn er **58** beveiligingsincidenten[123] gemeld. Daarvan zijn er **43** als datalek gekwalificeerd en intern geregistreerd, van die 43 datalekken zijn er **6** gemeld bij de Autoriteit Persoonsgegevens en daarvan zijn **5** datalekken gecommuniceerd naar de betrokkenen.

De overige beveiligingsincidenten zijn **1)** niet te kwalificeren als datalek; **2)** is de RUG niet de verantwoordelijke[124] of **3)** worden nog onderzocht.

De behandeling van datalekken wordt sinds het einde van 2020 in TOPdesk uitgevoerd. Evalueer in 2021 de effectiviteit van de procedure in het nieuwe systeem en de voorgestelde maatregelen.

De beoordeling van alle beveiligingsincidenten gebeurt binnen de RUG door de FG. Hierover adviseert hij het CvB. De incidenten met een middel of hoog risicoprofiel hebben prioriteit.[125] Advisering omtrent datalekken met een laag risicoprofiel laten in sommige gevallen enkele weken op zich wachten.[126] Dit is niet wenselijk.

De verwachting is dat de komende jaren het aantal gemelde datalekken gaat stijgen. 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.

Incidenten worden op dit moment vaak niet herkend en/of gemeld als inbreuk in verband met persoonsgegevens. Dit geldt zeker ook voor het domein onderzoek.

[123] Dit zijn mogelijke datalekken; verder onderzoek bij de RUG wijst uit of een incident ook een datalek is.
[124] Er zijn datalekken gekwalificeerd waarbij het Martini Ziekenhuis, een stichting of derde de verantwoordelijke is.
[125] Datalekken met een middel of hoog risicoprofiel worden gemeld bij de Autoriteit Persoonsgegevens (“AP”) respectievelijk de AP en de betrokkenen.
[126] Datalekken met een laag risicoprofiel worden enkel intern gedocumenteerd.

Datalekken in onderzoek

Vanuit het domein onderzoek zijn vijf datalekken gemeld. Gezien het grote aantal[127] onderzoeken met persoonsgegevens duidt dit eerder op het gebrek aan kennis over datalekken en de melding ervan dan op ondoordringbare beveiliging.

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.

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.[128] Die bewustwording kan al plaatsvinden bij de graduate school.

[127] Op elk gegeven moment worden er binnen de RUG meer dan 1000 onderzoeken met persoonsgegevens uitgevoerd. Exacte aantallen zijn niet bekend, omdat de registratie niet volledig is (zie ook hoofdstuk 6).
[128] 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 2020 had de coronacrisis een grote impact op de manier waarop we zijn gaan werken en daarmee ook op de manier waarop we persoonsgegevens verwerkten. Desondanks is een verdere inbedding van het privacybeleid in de organisatie te zien. Het volwassenheidsniveau van de privacymanagementorganisatie is gegroeid van 1,7 naar 2,1. De omvang en structuur van de organisatie, maar ook de diversiteit van de taken maakt dit geen eenvoudige stap.

Naast de bestuurders en directies hebben collega's als de privacy- & securitycoördinatoren veel werk verzet. De domeinen Onderwijs, Onderzoek en Bedrijfsvoering hebben zich verenigd en kunnen toewerken naar uniforme processen in 2021. Concrete plannen om dit te bereiken zijn in 2020 opgesteld. In 2021 is een start gemaakt.

De (ondersteunende) diensten vragen net als in 2019 nog aandacht. In 2021 moeten zij (meer) aandacht besteden aan hun Werkplannen. Daarin dienen de verwerkingen met de hoogste risico's worden benoemd. Ook een realistische planning is vereist om de risico's te mitigeren. Faculteiten moeten immers kunnen vertrouwen op de verwerking van persoonsgegevens in de gefaciliteerde processen en systemen.

Binnen het domein onderzoek is al meer aandacht voor de ondersteuning van de onderzoeker. Bewustwording en kennis, maar ook praktische maatregelen zijn nodig. Het GDCC gaat hierin een belangrijke rol spelen, maar decentrale ondersteuning blijft onmisbaar. De kennisdeling tussen ethische commissies is daarom ook een positieve ontwikkeling.

Naast de interne organisatie, is er meer contact met betrokkenen over de verwerking van hun persoonsgegevens. De omgang met die betrokkenen is organisatiebreed op een eenduidige wijze vastgelegd, wat de kwaliteit ten goede komt.

Voor verdere groei is focus op risicomanagement en "privacy by design" zeer gewenst. Toewijding van het CvB, directies en faculteitsbesturen blijft daarbij essentieel.

Bijlage 1. 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.