rijksuniversiteit groningen

Jaarverslag bescherming persoonsgegevens 2021

mr. A.R. Deenen | Functionaris voor de Gegevensbescherming

Vertrouwen in onderwijs en wetenschap door zorgvuldig omgaan met gegevens

Het Jaarverslag bescherming persoonsgegevens informeert en signaleert, maar geeft ook advies voor verdere verbetering. De focus ligt op de hoogste risico's en de daarbij voorgestelde maatregelen. De RUG is een grote en brede organisatie die de verbinding zoekt in de regio, maar zeker ook internationaal. Dit vraagt om een passende omgang met persoonsgegevens. In lijn daarmee zijn er drie belangrijke thema's te destilleren: 1) Excellent onderzoek met oog voor de mens; 2) Vergroten van kennis bij medewerkers; en 3) Risicomanagement in de keten. Na het jaarverslag 2020 zijn door het CvB meerdere maatregelen opgenomen in een programmaplan, maar hebben nog niet geresulteerd in een groei van de volwassenheid. De RUG blijft staan op een gemiddelde van **2,1**.[1]

De bedoeling van de AVG is niet om de verwerking van persoonsgegevens te verbieden, maar om bij de verwerking rekening te houden met de studenten, medewerkers en onderzoeksdeelnemers waarvan we de gegevens verwerken en om dat proces te bewaken.

1 Privacybeleid en inbedding in de organisatie

De ontwikkeling van de privacymanagementorganisatie kwam tot stilstand gedurende de coronacrisis. Wél schreven alle faculteiten en diensten een Werkplan privacy en security; deze plannen toonden bewustzijn ten aanzien van gegevensbescherming. Alle werkplannen zijn centraal beoordeeld.[2]
(●) goed (●) matig (●) onvoldoende/afwezig

Faculteit Rechtsgeleerdheid	●	Faculteit Gedrags- en Maatschappijwetenschappen	●
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 – domein onderzoek	●
Honours College	●		
Facilitair bedrijf	●	Het Bureau	●
Centrum voor Informatie Technologie	●	Universiteitsbibliotheek	●

Verder werd een programmamanager aangesteld en het Programma veilig en vertrouwd geschreven met als doel de volwassenheid van de universiteit in korte tijd (twee jaar) te verhogen.

(●) Aandachtspunt voor de RUG blijft de kennisontwikkeling in de eerste en tweede lijn; zowel mensen op de werkvloer als het management hebben voldoende kennis nodig om *privacy* te borgen en te adresseren in de organisatie.

---

[1] Het volwassenheidsniveau is vastgesteld aan de hand van de privacy assessment tool van het Centrum Informatiebeveiliging en Privacybescherming.
[2] De beoordeling vindt jaarlijks plaats door de Chief Information Security Officer, Chief Privacy Officer, IT-auditor en de Functionaris Gegevensbescherming.

2 Risicomanagement

Binnen de RUG is risicomanagement nog geen cyclisch proces en daarom is zij in de afgelopen drie jaren niet gegroeid op dit cruciale onderdeel. De beoordeling van risico's en het wegnemen van de hoogste risico's is niet ingebed in de opzet van (nieuwe) processen. Een belangrijke oorzaak is het ontbreken van "eigenaarschap" op data en processen. Er mist derhalve een entiteit die verantwoordelijk is voor de structurele beoordeling van risico's bij het ontwerp of de start van (nieuwe) processen.

Risicomanagement wordt naar een hoger plan getild door het aanwijzen en beschrijven van verantwoordelijkheden. Daarbij is het tijdig toepassen van Privacy by Design cruciaal.
Ook 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 universiteit zelf. Een positief neveneffect van een DPIA is kennisvergroting bij de deelnemers. Voor wetenschappelijk onderzoek kan het, in 2021 gestarte, Digital Competence Centre ("DCC") hierbij ondersteunen.

Aanbeveling: maak het DPIA structureel onderdeel van het opzetten van nieuwe processen en systemen. Een DPIA wijst (hoge) risico's aan en levert passende maatregelen op, maar maakt processen ook inzichtelijk.
Zorg daarnaast voor voldoende zichtbaarheid en bemensing van het DCC.

3 Kwaliteitsmanagement

Hoe borgen we als universiteit dat de gegevens waar we mee werken correct zijn en hoe corrigeren we deze indien nodig; dat is waar kwaliteitsmanagement over gaat. Concreet: woont een student nog steeds op hetzelfde adres en is een alumnus nog wel op het geregistreerde e-mailadres bereikbaar? Ook het kunnen rectificeren, aanvullen, verwijderen en beperken van de verwerking van persoonsgegevens valt hieronder. Dit is binnen de RUG behoorlijk geregeld. Zij profiteert daarbij van de onderwijsketen[3].
Het bewaken van de juistheid van persoonsgegevens vraagt vooral aandacht verderop in de interne procesketen (lees: verder af van de bronsystemen). Gegevens toegankelijker maken voor betrokkenen helpt daarbij; zij kunnen dan te allen tijde relevante wijzigingen doorgeven.

4 Register

Weten wat je als organisatie met persoonsgegevens doet en waar, is onderdeel van de verantwoordingsplicht. De RUG heeft daarom een register van verwerkingsactiviteiten ("register"). Het register is een middel om tot eenduidige en zorgvuldige verwerkingen te komen. Met een actueel en volledig register kan de RUG beter sturen op risico's. De RUG is nog niet op dat punt aanbeland. Tot op zekere hoogte is er inzicht in de verwerkingen van persoonsgegevens binnen de domeinen Onderwijs en Bedrijfsvoering. Dit zijn echter procesregistraties die veelal verouderd zijn. Ook vormt het register nog geen volledig beeld van alle verwerkingen binnen de instelling. Zonder een actueel en volledig beeld is het nog lastig sturen op risico's en daarmee op het maatschappelijk verantwoord omgaan met data.

[3] Denk aan de borging van datakwaliteit bij Studielink.

Voor het domein Onderzoek is centraal niet vastgesteld hoe onderzoek met persoonsgegevens inzichtelijk moet worden gemaakt. De voorkeur heeft een (decentrale) procedure die in lijn ligt met het datamanagementbeleid en gedeelde verantwoordelijkheden verheldert. Daarbij kan het beschrijven van disciplinespecifieke onderzoeksscenario's met maatregelen veel overbodig werk voorkomen.
In 2022 is de RUG voornemens om alle beschreven processen met persoonsgegevens online te publiceren. Met dit real-time overzicht werkt de RUG op een vooruitstrevende wijze toe naar transparantie.

5 Doelbinding en intern toezicht

Uit het Strategisch Plan 2021-2026 wordt duidelijk welke doelen de Groninger universiteit heeft. Om deze doelen op een maatschappelijk verantwoorde wijze te behalen zijn persoonsgegevens onmisbaar. Eén van de kaders uit de AVG is "doelbinding"; gegevens enkel verwerken voor het doel waarvoor ze initieel zijn verzameld. Het bewaken van doelbinding vindt idealiter plaats in de gehele organisatie.
Binnen de diensten en faculteiten worden doelen veelal nog informeel bepaald en is uniformering beperkt aanwezig. Waar facultaire verwerkingen op elkaar lijken, lopen de doelen uiteen en wijken deze af van hetgeen naar studenten en medewerkers wordt gecommuniceerd.

Aanbeveling: bereik effectieve controle op de doelen van verwerkingen door zoveel mogelijk op centraal niveau doelen en de wijze van verwerken vast te stellen. Daarbij dienen de instellingsbrede doelen te worden gekoppeld aan gestandaardiseerde processen binnen de RUG.

Toezicht en positionering FG

Binnen de RUG kan de FG zijn werk onafhankelijk uitvoeren, wat organisatorisch is geborgd. Sinds 2020 is de FG lid van de Strategische Commissie Privacy en Security; een periodiek overleg met vertegenwoordiging vanuit het CvB, faculteitsbesturen en directies. Verder zijn er structurele overleggen met de Chief Privacy Officer en heeft de FG middelen tot zijn beschikking voor verdere opleiding. Daarentegen heeft de Raad van Toezicht zich sinds 2019 niet meer (fysiek) laten informeren door de FG, ondanks verzoeken van zijn kant. Leden van de universiteits- en faculteitsraden weten de FG wel goed te vinden, net als studenten en onderzoeksdeelnemers. Bij het wetenschappelijk personeel is de FG minder bekend.

6 Bewaren van persoonsgegevens en opslagbeperking

Het streven is om persoonsgegevens niet langer te bewaren dan noodzakelijk is voor de doelen waarvoor deze zijn verzameld. Binnen de RUG zijn in 2020 stappen gezet om bewaartermijnen beter na te leven. 2021 kende een stilstand, maar met de inzet van de archivaris én het Programma veilig en vertrouwd wordt het borgen van bewaartermijnen naar een hoger niveau getild in 2022/2023.

Een punt van aandacht zijn de veel gebruikte media, zoals e-mail en berichtenapps. Deze kennen geen bewaartermijnen, maar vormen wel een ongestructureerd en moeilijk beheersbare opslag van persoonsgegevens. Wanneer (werk)processen duidelijk zijn, kunnen gegevens op de daarvoor bedoelde plaatsen worden bewaard en uit de e-mail en apps worden verwijderd.
Voor het vaststellen van bewaartermijnen in onderzoek is het aan te raden om binnen de verschillende disciplines aansluiting te zoeken bij de landelijke netwerken (en disciplinespecifieke richtlijnen).

7 Beveiligen van persoonsgegevens

De Roadmap informatiebeveiliging 2020-2021 kende een groot aantal lopende projecten met beperkte of onduidelijke voortgang. De organisatie van informatiebeveiligers kent grote uitdagingen bij het vasthouden en aantrekken van nieuwe krachten. Met een tekort aan specialisten op het gebied van informatiebeveiliging is het intern opleiden van P&S-coördinatoren niet tot nauwelijks gebeurd. Verder was informatiebeveiliging geen integraal onderdeel bij de opzet van veel nieuwe processen/systemen. Dit geldt voor alle faculteiten en diensten binnen de RUG, inclusief het CIT. Verder zijn periodieke risicoanalyses momenteel schaars. Met het aanstellen van de CISO in 2020 heeft informatiebeveiliging wel een hogere prioriteit gekregen binnen de organisatie. Wel lijkt informatiebeveiliging op dit moment nog een aangelegenheid te zijn van het CIT. Het gaat echter om informatiebeveiliging en niet om ICT-beveiliging.

Aanbevelingen: werk toe naar een onafhankelijke CISO die verantwoording aflegt aan het CvB en breng P&S-coördinatoren basiskennis bij over informatiebeveiliging.
Verder is het noodzakelijk om onderzoekers te ondersteunen bij informatiebeveiliging in middelen en kennis. Het DCC kan daarbij een belangrijke rol spelen. Ook initiatieven als de Virtual Research Workspace zijn belangrijk maar bieden nog een te beperkte dienstverlening.

8 Informatieverstrekking en rechten betrokkenen

Transparantie is één van de pijlers binnen gegevensbescherming. 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. De manier waarop de RUG hiermee omgaat schept vertrouwen en is degelijk neergezet.

9 Verwerkers en doorgifte

Bij de verwerking van persoonsgegevens zet de RUG honderden organisaties in, de “verwerkers”. Deze verwerkers dienen een passend beschermingsniveau te hanteren. Dit geldt ook wanneer deze verwerkers zich buiten de Europese Unie bevinden, wat een uitdaging voor de RUG vormt.
Naast de verwerkers kent de RUG veel complexe samenwerkingsverbanden binnen het wetenschappelijk onderzoek en onderwijs. Afspraken over (gezamenlijke) gegevensbescherming zijn echter nog geen standaard in het veld en vragen binnen de RUG om een duidelijke verdeling van verantwoordelijkheden. Wie ziet namelijk toe op de gegevensbescherming en hoe?

Aanbeveling: leg vast hoe de RUG omgaat met doorgifte van gegevens naar het buitenland en borg dat proces.

10 Datalekken

Het aantal gemelde incidenten (**34**) blijft stabiel. Van die incidenten zijn er **21** als datalek gekwalificeerd. Het overgrote deel daarvan is een datalek met een laag risico voor de betrokkenen en universiteit. Denk daarbij aan het delen van een cijferlijst waarop medestudenten staan vermeld. Er is **één** datalek gemeld bij de Autoriteit Persoonsgegevens.

Aanbeveling: draag zorg voor een grondige opvolging van de voorgestelde maatregelen om toekomstige datalekken te beperken.

Vooruit(kijken)

De stilstand in groei op dit thema lijkt een tijdelijke. Eind 2021 heeft het CvB akkoord gegeven op een integraal en uitgebreid programma om de omgang met gegevensbescherming én informatiebeveiliging binnen de organisatie op alle domeinen te verhogen. Hierin is tevens het onderwijs van personeel meegenomen; een zorgvuldige omgang met persoonsgegevens begint namelijk op de werkvloer. Verder vergroot de RUG de transparantie naar betrokkenen toe door haar register van verwerkingen online te publiceren en “realtime” bij te houden.

Voor het wetenschappelijk onderzoek doen het CvB en het College van Decanen er goed aan om (decentrale) best practices beter te ondersteunen en bekend te maken bij het wetenschappelijk personeel. De inzet en structurele inbedding van het DCC helpt daarbij.