rijksuniversiteit groningen

Jaarverslag bescherming persoonsgegevens 2023

Functionaris voor de gegevensbescherming

mr. A.R. Deenen

Vertrouwen in onderwijs en wetenschap door zorgvuldig omgaan met gegevens

Het *Jaarverslag bescherming persoonsgegevens* schetst de omgang met persoonsgegevens binnen de RUG en bevat aanbevelingen. De nadruk ligt op de grootste risico's en de daarmee samenhangende maatregelen. De functionaris gegevensbescherming ("FG") gaat daarbij dit jaar uit van drie thema's: 1) excellent onderzoek met aandacht voor de mens; 2) vergroting van kennis onder medewerkers; en 3) risicomanagement in de keten. Na de start van het Programma Veilig en Vertrouwd in 2022 zijn in 2023 belangrijke besluiten over de governance, risicomanagement en awareness genomen. Deze komen terug in de verschillende hoofdstukken.

De werkzaamheden binnen het Programma droegen bij aan een zichtbare groei van de volwassenheid van de RUG, met een gemiddeld niveau van **2,5**.[1]

Anders dan voorgaande jaren heeft de FG in het jaarverslag niet specifiek de concrete stappen beschreven die genomen dienen te worden om het volwassenheidsniveau te verhogen. De reden hiervoor ligt in de verbetering van de zogeheten *privacymanagementorganisatie*. Met de goede positionering van de P&S-coördinatoren, Chief Information Security Officer ("CISO"), Chief Privacy Officer ("CPO") en andere functionarissen in de eerste en tweede lijn[2] wordt de voorgestelde koers al bepaald en wel met succes. Dit is een belangrijk compliment voor de organisatie.

De RUG heeft over de hele linie meer aandacht voor de zorgvuldige omgang met gegevens van studenten, medewerkers en onderzoeksdeelnemers. Bewustwording van dit onderwerp is op alle niveaus binnen de RUG toegenomen. Dit is terug te zien in de ontwikkelingen beschreven in de volgende hoofdstukken. Desalniettemin blijft de FG kritisch kijken naar mogelijkheden tot verbetering.

[1] In 2022 werd bij de RUG nog een volwassenheidsniveau van 2,4 vastgesteld. Het volwassenheidsniveau is vastgesteld aan de hand van de privacy assessment tool van het Centrum Informatiebeveiliging en Privacybescherming.
[2] Het 'Three lines-model' beschrijft de wijze waarop controle op processen plaatsvindt. De *eerste lijn* bestaat uit de mensen op de werkvloer, inclusief het management, die gegevens verwerken. De *tweede lijn* is de controlerende en adviserende groep voor de eerstelijn en bestaat uit P&S-coördinatoren, privacyjuristen en Chief Privacy Officer. De *derde lijn* bestaat uit een onafhankelijke toezichthouder zoals de accountant en de FG.

1 Privacybeleid en inbedding in de organisatie

Met de implementatie van het Programma Veilig en Vertrouwd ("het Programma") is concreet invulling gegeven aan een sleutelfiguur binnen het domein van gegevensbescherming (privacy) en informatiebeveiliging, namelijk de P&S-coördinator. Er is een functieprofiel opgesteld en goedgekeurd, waarin de positie, taken en verantwoordelijkheden helder zijn uiteengezet. Daarnaast is besloten dat de P&S-coördinator tijd reserveert voor betrokkenheid bij organisatiebrede thema's en verwerkingen in het P&S-Gilde ("Gilde"). Door de samenwerking in het Gilde wordt voorkomen dat hetzelfde proces op verschillende plekken wordt herhaald, waarmee tegemoet wordt gekomen aan zorgen vanuit de faculteiten over dubbel werk. Op enkele uitzonderingen na heeft de P&S-coördinator bij elke faculteit/dienst voldoende formatie voor zijn werk.[3] Dit is terug te zien in de opgestelde P&S-Werkplannen ("Werkplannen") van de faculteiten en diensten.[4]

Format Werkplan Privacy & Security

De faculteiten en diensten hebben dit jaar een nieuw format Werkplan ontvangen om mee te werken. Dit leidde enerzijds tot een meer concrete beschrijving van de risico's, wat gegevensbescherming en informatiebeveiliging tastbaarder maakt. Anderzijds was het detailniveau dermate groot dat Werkplannen voor faculteitsbestuurders en directies moeilijk leesbaar waren. De CISO en CPO hebben de feedback met betrekking tot de Werkplannen ter harte genomen en zoeken voor aankomend jaar naar een evenwichtige werk- en rapportagevorm.

Acties vanuit het Programma Veilig en Vertrouwd

Verder zijn vanuit het Programma de analyses van de *business impact* ("BIA") bij de faculteiten en diensten grotendeels afgerond. De business impact-analyse beschrijft welke processen binnen een faculteit en dienst kritisch zijn en welke maatregelen daaraan gekoppeld (moeten) worden om nadelige gevolgen te voorkomen. Denk hierbij aan het uitvallen van de e-mail, diefstal van intellectueel eigendom of storing in de uitbetaling van salarissen.

Ondanks de goedkeuring van meerdere acties in het Programma in het eerste kwartaal van 2023, zijn een aantal zaken niet of niet voortvarend uitgevoerd. Hieronder valt het structureel aanstellen van een awareness- en trainingscoördinator, het voldoende faciliteren van het software-aanvraagproces, het formaliseren van de positie van de CPO en het opnemen van structurele kosten in de begroting om in volwassenheid te groeien tot 3.0. In tegenstelling tot het voorgaande heeft het College van Bestuur wel duidelijk gecommuniceerd naar de faculteiten en diensten dat bezuinigingen op de personeelsformatie voor P&S-activiteiten niet waren toegestaan.

Daarnaast heeft het Programma diverse campagnes gelanceerd om medewerkers en studenten bewust te maken van het belang van beveiliging en gegevensbescherming (privacy). Naast posters en nieuwsbrieven omvat dit ook Podcasts, lezingen en trainingen.

Verantwoordelijkheden in onderzoek

Gegevensbescherming binnen onderzoek vormt een complex en veranderlijk landschap, waarbij diverse invalshoeken, waaronder privacy, beveiliging, ethiek en gegevensbeheer, elkaar beïnvloeden. Ondanks schijnbare nauwe samenwerking ontbreekt in werkelijkheid een geïntegreerde aanpak in de procedures rondom gegevensbescherming. Met name op tactisch en strategisch niveau dient door faculteiten samen met het DCC toegewerkt te worden naar een multidimensionale benadering.

[3] Dit zijn de Faculteit Science and Engineering, het CIT, UCG, Campus Fryslân, UMCG en het Cluster R&I.
[4] In het P&S-Werkplan worden processen en risico's beschreven, maatregelen geformuleerd en geëvalueerd.

Model van eigenaarschap

Als laatste is een belangrijk model van eigenaarschap omarmd en geaccordeerd. Binnen dit model wordt een duidelijk onderscheid gemaakt tussen de risico-eigenaar, de proceseigenaar, de systeemeigenaar en de data-eigenaar. Binnen de RUG is de expliciete vastlegging van verantwoordelijkheden vaak ontoereikend. Door het eigenaarschap concreet te definiëren, worden grijze gebieden, hiaten en besluiteloosheid weggenomen. Het wordt helder wie welke verantwoordelijkheid draagt bij het vergroten van de volwassenheid van processen en de organisatie. De implementatie van het model van eigenaarschap vergt tijd en betrokkenheid van de faculteitsbestuurders en directies.

Aanbeveling

- Implementeer het model van eigenaarschap om expliciete verantwoordelijkheden vast te leggen en helderheid te verschaffen binnen de RUG, met specifieke betrokkenheid van faculteitsbestuurders en directies.
- Draag zorg voor regelmatige consultatie van het DCC door het college van decanen; zo kan met hun advies gegevensbescherming op tactisch en strategisch niveau worden verbeterd.

2 Risicomanagement

Het beheer van risico's begint met beleid en het beleggen van verantwoordelijkheden. In navolging van het Programma ligt er een duidelijke blauwdruk om intern de juiste verantwoordelijkheden te beleggen. Onderscheid is hierbij gemaakt tussen risico-, systeem-, proces- en data-eigenaar. Waar het model logisch en duidelijk is, vraagt de toepassing enige toewijding van bestuurders en directies, want bij de RUG bestaan er veel grijze gebieden. Ondersteunend aan de eigenaren is de P&S-organisatie[5]. De P&S-organisatie is uitdrukkelijk geen eigenaar van de hiervoor vermelde processen, wat in de praktijk weleens wordt vergeten.

Training P&S-coördinatoren en Werkplannen

Naast de governance zijn er veel trainingen risicomanagement verzorgd voor de P&S-coördinatoren. En met succes; de opgeleverde Werkplannen toonden een groter inzicht in risico's en de wijze waarop die gemitigeerd moeten worden (zie hoofdstuk 1). De Werkplannen vormen de kern van het risicomanagement bij de universiteit en worden opgesteld door de faculteitsbesturen en directies. Zij leggen verantwoording af over hun beleid en werkzaamheden met betrekking tot gegevensbescherming aan het CvB. In de Werkplannen zijn dit jaar tevens de nulmetingen gegevensbescherming & informatiebeveiliging van Deloitte meegenomen die hebben plaatsgevonden binnen de gehele RUG. Deloitte toonde daarmee ook de risico's per faculteit/dienst. Faculteiten en diensten konden meteen aan de slag.

DPIA en training nieuwe medewerkers

Afgezien van de PDCA-cyclus[6] met de Werkplannen, is er ook een verandering merkbaar in de aanpak van risico-assessments (DPIA[7]) bij nieuwe of gewijzigde verwerkingen van persoonsgegevens. Proceseigenaren pakken in samenwerking met de P&S-coördinator vaker en tijdig het traject op. Een DPIA biedt een concreet overzicht van risico's, vergezeld met een reeks aan maatregelen die toepasbaar is binnen de gehele organisatie.[8] Bij de behandeling van organisatiebrede DPIA's spelen

[5] Hieronder vallen onder meer de privacy- en securitycoördinatoren ("P&S-coördinatoren"), Chief Privacy Officer ("CPO"), Chief Information Security Officer ("CISO"), privacyjuristen en Information Security Officers.
[6] Een Plan Do Check Act-cyclus is een continu verbeteringsproces om processen efficiënter en effectiever te maken.
[7] Data Protection Impact Assessment.
[8] Een voorbeeld hiervan is het DPIA op collegeregistraties.

het CvB én de universiteitsraad een rol; dit benadrukt het belang van gegevensbescherming als essentieel onderdeel van het beleid binnen de instelling.

Tenslotte is er een belangrijk besluit genomen door de Stuurgroep van het Programma. De trainingen met betrekking tot gegevensbescherming en informatiebeveiliging worden verplicht voor nieuwe medewerkers. Voor bestaande medewerkers is deelname aan de training optioneel, maar wordt wel sterk aanbevolen.

Aanbeveling

Zorg ervoor dat gegevensbescherming en de evaluatie van de Werkplannen door het College van Bestuur standaard op de agenda staan van het bestuurlijk overleg.

3 Kwaliteitsmanagement

Bij kwaliteitsmanagement binnen gegevensbescherming (privacy) hebben we het over processen die zorgdragen voor correcte, betrouwbare en volledige data. Daarbij hoort dus het actueel houden van gegevens. Denk bijvoorbeeld aan het tijdig en correct wijzigen van het adres van een medewerker na een verhuizing, zodat zij of hij vertrouwelijke post op het goede adres ontvangt. Of het kunnen onderhouden van goede communicatie met alumni. Zonder kwaliteitsmanagement leidt wetenschappelijk onderzoek tot de verkeerde of ongewenste resultaten. Of medewerkers en studenten ervaren een slechte dienstverlening of worden zelfs benadeeld.

Eigenaarschap binnen kwaliteitsmanagement

Op het gebied van kwaliteitsmanagement binnen de RUG zijn verschillen waarneembaar tussen de diverse domeinen. Bij wetenschappelijk onderzoek, waar datamanagementplannen worden gehanteerd, vormt datakwaliteit een onmisbaar aspect van het onderzoek. Daarentegen lijkt binnen de bedrijfsvoering de datakwaliteit een minder grote prioriteit te hebben. De onbekendheid met verantwoordelijkheden, zoals beschreven in hoofdstuk 2 Risicomanagement, maakt dat afdelingen/medewerkers zich onterecht hiervoor niet verantwoordelijk voelen. Daar is binnen het Programma aandacht aan besteed door te focussen op het ‘eigenaarschap’. Dit concept is omarmd door het Programma, maar het zogenaamde *bestaan* en vooral de *werking* zijn binnen belangrijke processen nog niet aantoonbaar aanwezig.

Onderwijsprocessen profiteren wat betreft datakwaliteit van een goede en actuele koppeling met ketenpartners als Studielink; er wordt gestreefd naar een hoge datakwaliteit in de zogenaamde bronsystemen.

Het waarborgen van datakwaliteit, ook wel de “juistheid van persoonsgegevens” vereist heldere verantwoordelijkheden (eigenaarschap) en aandacht bij de opzet van processen. Datakwaliteit is om die reden een vast onderdeel van het DPIA-format[9] van de RUG. Daarnaast draagt het faciliteren van toegang tot gegevens van betrokkenen (o.a. studenten, medewerkers, alumni) bij aan het actueel en correct houden van de gegevens.

[9] Bij een Data Protection Impact Assessment wordt gekeken naar de risico’s in een (nieuw) proces en worden passende maatregelen beschreven om de impact op mensen en de organisatie weg te nemen of te verkleinen.

4 Register

Binnen de RUG is een degelijk proces aanwezig om (nieuwe) verwerkingen te beschrijven en te controleren in het register. De faculteiten en diensten zijn verantwoordelijk voor het beschrijven en het centrale privacyteam heeft daarbij een controlerende taak. De meerwaarde van de centrale controle zit hem in het verbeteren van verwerkingen - kan het proces sneller lopen met minder gegevens - en kan er regie plaatsvinden op het uniformeren van processen. Door deze centrale regie hoeft niet elke faculteit het wiel opnieuw uit te vinden.

Completeren van het register

Het register geeft een overzicht van verwerkingen van persoonsgegevens verdeeld over de faculteiten en diensten. Binnen de faculteiten en diensten zijn de P&S-coördinatoren vaak initiator van het optekenen van nieuwe en gewijzigde verwerkingen; dit naar aanleiding van nieuwe overeenkomsten, DPIA's of zelfs incidenten. Met dank aan de P&S-coördinator van de Faculteit Rechtsgeleerdheid zijn in september meerdere studentassistenten gestart om de achterstand in beschreven verwerkingen weg te werken bij de faculteiten en diensten.

De RUG heeft het register sinds 2022 gepubliceerd op haar website en vormt daarmee een goed voorbeeld in de branche en daarbuiten. Met het register wordt richting zowel de toezichthouder (Autoriteit Persoonsgegevens) als de betrokkenen getoond wat de RUG met persoonsgegevens doet.

Verwerkingen binnen wetenschappelijk onderzoek

Aandachtspunt blijft het in kaart brengen van de verwerkingen binnen wetenschappelijk onderzoek. Waar veel onderzoeken wel in beeld zijn door middel van datamanagementplannen, ethische toetsing of financiële controle, is er geen eenduidige wijze waarop onderzoek wordt geregistreerd. Begin 2024 heeft de FG de Rector Magnificus een advies toegezonden waarin enkele randvoorwaarden worden beschreven voor een goede registratie van onderzoek. De kern van het advies luidt: sluit aan bij bestaande processen om onderzoek met persoonsgegevens in kaart te brengen. Een extra drempel creëren voor onderzoekers is niet wenselijk, maar ook niet nodig. Een goed gestructureerd proces kan onderzoekers zelfs helpen bij het toepassen van gegevensbescherming, informatiebeveiliging en open science in de onderzoeksopzet door middel van zogeheten 'building blocks'.[10]

Werk toe naar uniforme processen om wetenschappelijk onderzoek met persoonsgegevens in kaart te brengen. Hanteer daarbij de eerder geadviseerde randvoorwaarden.

Aanbeveling

5 Doelbinding en intern toezicht

Persoonsgegevens gebruiken voor het doel waarvoor je ze initieel hebt verzameld, dat is doelbinding. Dit beginsel vormt een van de fundamenten van gegevensbescherming. Het betekent dat gegevens in principe niet worden gebruikt voor andere doeleinden. Gegevens binnen onderwijsprocessen worden daarom niet zomaar ingezet voor marketingdoeleinden en gegevens in personeelsdossiers worden niet zomaar gedeeld met een IT-leverancier om het product of de dienst te verbeteren.

De universiteit heeft de doelen waarvoor zij persoonsgegevens verwerkt beschreven in het register en update deze informatie periodiek. Zoals in hoofdstuk 4 al werd beschreven worden verwerkingen

[10] Dit zijn sets aan (beveiligings)maatregelen voor onderzoek zoals de pseudonimiseringsdienst, versleutelen van opslagmedia, data veilig koppelen, Research Data Management System en de Virtual Research Workspace.

van faculteiten en diensten gecontroleerd op een aantal beginselen. Hier valt ook de doelbinding onder en deze wordt dus ook afgedwongen door het centrale privacyteam, de zogeheten tweede lijn. Het gebruik van het register leidt daarmee tot een uniforme en vastgestelde wijze van gebruik van persoonsgegevens voor gerechtvaardigde doelen en biedt de FG een middel om toe te zien op correct gebruik van de gegevens voor die (gerechtvaardigde) doelen. Op het vlak van doelbinding is de RUG dan ook gegroeid ten opzichte van het voorgaande jaar.

Toezicht en positionering FG

De FG geeft advies en verstrekt informatie aan het (hoger) management, waaronder de directies, faculteitsbestuurders en de leden van het College van Bestuur. Binnen de RUG voert de FG deze taken uit zonder daarbij van iemand instructies te ontvangen, dit is conform wet- en regelgeving.

Net als in het voorgaande jaar vond structureel overleg plaats tussen de CPO, CISO en de FG. Ook was er een goede communicatielijn tussen de programmamanager van het Programma en de FG. Op die manier kon de FG zien en beoordelen of de RUG op de juiste manier werkte aan een zorgvuldige omgang met de gegevens van studenten, medewerkers en onderzoeksdeelnemers. Dit was het geval.

Ondersteuning en werkzaamheden

In aanvulling op de communicatielijnen heeft de FG, na zijn verzoek, structureel (secretariële) ondersteuning gekregen. Hierdoor heeft de FG voldoende ruimte gekregen om zijn werk naar behoren te kunnen uitvoeren. Daarnaast heeft de FG de beheerstaken binnen het datalekkenproces overgedragen aan de CPO. Daarmee zijn de taken beter gescheiden en voert de FG praktisch geen tweedelijnswerkzaamheden meer uit.

Dat werk omvatte afgelopen jaar onder meer de beoordeling en terugkoppeling van alle Privacy & Security Werkplannen van de faculteiten en diensten. Daarnaast heeft de FG meegekeken en geadviseerd bij een aantal DPIA's, waaronder die op het Career & Alumni platform, Opnamevoorzieningen in collegezalen en Hora Finita.

Verder heeft de FG meermalen gesproken met de leden van het CvB. Dit waren evenwichtige gesprekken die verduidelijking brachten voor beide partijen. Waar alle belangen open op tafel liggen, kan de FG het beste adviseren. De meeste adviezen van de FG zijn binnen de instelling opgevolgd. Een aantal adviezen is, zonder toelichting of weerlegging niet of nog niet gevolgd.[11]

Wat bij de FG zelf is blijven liggen is de audit op Brightspace, welke in 2023 niet is afgerond; dit komt onder meer door andere prioriteiten van de FG en het vertrek van de IT-auditor.

Raad van toezicht & gegevensbescherming

Tot slot, een beknopt bericht met betrekking tot de Raad van Toezicht ("RvT"). De RvT doet er verstandig aan om een blik te werpen op de handreiking van de Autoriteit Persoonsgegevens.[12] Daarin staat hoe, met de Corporate Governance Code in de hand, gekeken kan worden naar

[11] Hieronder valt het advies ten aanzien van de inrichting van informatiebeveiliging binnen de RUG (zie hoofdstuk 7). Daarnaast het advies aan twee directeuren om een training gegevensbescherming te volgen zodat ook zij herkennen waar *Privacy by Design* nodig is. Het laatste advies was aan de afdeling Communicatie om het gebruik van cookies in lijn te brengen met de Telecommunicatiewet.

[12] 'De RvC of RvT en privacy: uw rol als toezichthouder', Autoriteit Persoonsgegevens, https://autoriteitpersoonsgegevens.nl/uploads/2023-12/Handreiking%20De%20RvC%20of%20RvT%20en%20privacy%20uw%20rol%20als%20toezichthouder.pdf, versie december 2023.

dataprotectie als lid van de RvT. Daarbij kan het bevorderlijk zijn voor de toezichtstaken om wel periodiek het gesprek aan te gaan met de FG.

6 Bewaren van persoonsgegevens en opslagbeperking

Binnen het ruime scala aan onderwerpen binnen het thema gegevensbescherming heeft 'opslagbeperking' nog aandacht nodig. Onder opslagbeperking wordt onder meer verstaan het niet langer bewaren van gegevens dan noodzakelijk om het initiële doel te bereiken, maar ook het archiveren en vernietigen van gegevens in overeenstemming met sectorspecifieke wetgeving. Naast de Algemene Verordening Gegevensbescherming ("AVG") heeft de RUG de Archiefwet te volgen en meer specifiek de zogenaamde *Selectielijst Universiteiten en Universitaire Medische Centra*. In de selectielijst staat het merendeel van processen binnen de universiteit beschreven en daarbij de verwijder- en bewaartermijnen. Dit geldt overigens niet voor wetenschappelijk onderzoek waar vaak disciplinespecifieke bewaartermijnen gelden. Een bewaartermijn van 10 jaar na afloop van het onderzoek wordt vaak genoemd, maar deze termijn wordt meer dan eens niet nageleefd.

Dataclassificatie

Wat het naleven van opslagbeperking binnen de RUG een uitdaging maakt is het classificeren van alle data. Dat houdt in dat bekend is met welk soort data gewerkt wordt en wat je daarmee wil of moet doen. Aan de hand van deze dataclassificatie zijn vervolgens beveiligingsmaatregelen en bewaartermijnen toe te passen. Dataclassificatie is binnen de RUG nog geen standaard onderdeel van de opzet van veel nieuwe processen. In de Werkplannen van de faculteiten en diensten wordt wel aandacht besteed aan dataclassificatie, maar dat levert nog geen organisatiebreed inzicht of controle op.

Structureel archiveren en verwijderen

Naast het gebrek aan dataclassificatie is het afgelopen jaar wederom beperkt aandacht geweest voor het gecontroleerd archiveren en verwijderen van gegevens. De afdeling Documentaire Informatievoorziening ('DIV') voert wel incidentele opruimacties uit, maar dat vormt slechts een fractie van hetgeen gearchiveerd/verwijderd dient te worden volgens de wet en de Selectielijst. Werkende processen om gegevens vanuit Brightspace en Progress.NET gecontroleerd te archiveren of te verwijderen zijn nog niet in bedrijf. Een duidelijk positieve noot vormt wel de Werkgroep Bewaartermijnen (van het Programma). Deze werkgroep heeft het adviesdocument *top 10 bewaartermijnen* opgeleverd. In lijn met dat document wordt momenteel gewerkt aan implementatie van bewaartermijnen in AFAS.

Beheer van de gezamenlijke schijven en apps

Naast voornoemde werkgroep is vanuit het Programma ook gezorgd voor een applicatie om de rechten op de Y-schijf inzichtelijk te maken. Een duidelijk overzicht ontbrak al jaren, dit is dus een grote stap vooruit. Met deze applicatie kunnen beheerders (en P&S-coördinatoren) overgaan tot beheer van de verschillende mappen op de Y-schijf. Tegelijkertijd is in 2023 bij University Services een start gemaakt met het proces om de Y-schijf op te ruimen en te herstructureren. Dit proces zal voortduren in 2024-2025 en na een (tussentijdse) evaluatie wordt deze nieuwe indeling en werkwijze organisatiebreed geïmplementeerd.

Onderdeel van het gecontroleerd archiveren en verwijderen van gegevens is het duurzaam opslaan en verwijderen van gegevens in communicatiemiddelen zoals e-mail en berichtenapps. Een dergelijk initiatief is nog niet in gang gezet waardoor een aanzienlijke hoeveelheid essentiële informatie verloren gaat, dan wel te lang (onveilig) bewaard blijft.

Informatiemanagement

Alles in overweging nemend valt op dat er centrale regie op informatiemanagement ontbreekt, waarbij de logische samenhang tussen informatiestromen, bedrijfsprocessen en organisatiedoelen niet voldoende is gewaarborgd. Dit is bevestigd door het adviesbureau VHIC. In juni 2023 heeft het CvB daarom besloten om sturing te geven aan de ontwikkeling van informatiebeheer en daarvoor een projectgroep in het leven geroepen die het plan van aanpak opstelt. Daarnaast gaat het inrichten van het eigenaarschap, zoals dit in het Programma is geformuleerd, en dataclassificatie helpen bij het tijdig vernietigen of archiveren van gegevens.

Aanbeveling

- Implementeer de archiverings- en vernietigingsprocessen binnen de grootste "stapelapplicaties" Brightspace, Progress.NET en AFAS.
- Voor het vaststellen van bewaartermijnen in het onderzoek wordt geadviseerd om aansluiting te zoeken bij de landelijke netwerken en discipline-specifieke richtlijnen.

7 Beveiligen van persoonsgegevens

Gegevensbescherming is praktisch onmogelijk zonder degelijke informatiebeveiliging. In beginsel dragen de faculteiten en diensten hiervoor de verantwoordelijkheid. Binnen de RUG bestaat echter onduidelijkheid over de verantwoordelijkheid voor informatiebeveiliging. Het wordt onterecht gelijkgesteld aan ICT-beveiliging. Dit belemmert een doeltreffende aanpak en leidt tot het toeschuiven van verantwoordelijkheden richting het CIT. Het is derhalve begrijpelijk dat KPMG adviseert[13] de Chief Information Security Officer ("CISO") en de Information Security Officers ("ISO") niet binnen de IT-organisatie te huisvesten. De FG heeft in lijn hiermee geadviseerd.[14]

Verbetering van processen

Binnen het Programma is het merendeel van de middelen richting de verbetering en volwassenheidsgroei van informatiebeveiliging gegaan. Naast een nulmeting van Deloitte bij alle faculteiten en diensten voor informatiebeveiliging, is gewerkt aan de opzet van assetmanagement[15], de procesinrichting *Inkoop derde partijen, Interne beheersing*[16] en zijn ITIL-processen[17] bij het CIT geïmplementeerd. Ook is het zogenaamde *Software Aanvraagproces* opgezet waardoor informatiebeveiliging en gegevensbescherming beter geborgd zijn bij de inkoop van (nieuwe) applicaties en hardware.

Training en nieuwe specialisten

Verder zijn er trainingen gegeven aan de P&S-coördinatoren, ISO's en privacyjuristen over risicomanagement en lopen de trainingen voor *Information Security Foundation* door in 2024. Ook zijn in het laatste kwartaal van 2023 een aantal ISO's en een CISO in dienst getreden en zijn een aantal gedetacheerde ISO's en CISO vertrokken. Deze wisseling kan bijdragen aan de continuïteit van informatiebeveiliging waar in de afgelopen jaren veel 'doorstroom' van personeel was.

[13] Governance van Cybersecurity, Privacy & Kennisveiligheid HO – Pas toe of leg uit!', KPMG en Platform Integrale Veiligheid Hoger Onderwijs, 15 juni 2020.
[14] Het CvB is afgeweken van dit advies en wil de positionering van de CISO over 3 jaren evalueren op, voor de FG, nog onbekende gronden.
[15] Het vastleggen van de "assets" (lees: apparatuur) om het te beheren en risico's te minimaliseren.
[16] De Interne Beheersing ziet op de controle vanuit de derde lijn, zoals de IT-auditor, die momenteel afwezig is.
[17] ITIL-processen omvatten best practices en gestandaardiseerde processen voor IT-servicemanagement om IT-diensten te optimaliseren en efficiëntie te verhogen, problemen te beheren en de algemene kwaliteit van IT-diensten te verbeteren.

Informatiebeveiliging binnen wetenschappelijk onderzoek

Tenslotte, binnen het wetenschappelijk onderzoek blijft er vraag naar passende technische en organisatorisch maatregelen om onderzoek (met gevoelige data) te kunnen uitvoeren. Het Digital Competence Center ("DCC") biedt hierin enige ondersteuning, maar voor onderzoekers blijft het initiële aanspreekpunt de facultaire onderzoeksondersteuning. De handvatten die deze onderzoeksondersteuning biedt wisselt sterk per faculteit. Derhalve worden niet alle onderzoekers tijdig en voldoende geholpen met passende maatregelen. Dit leidt tot onderzoek met geïmproviseerde maatregelen die onvoldoende de risico's binnen het onderzoek mitigeren.

Een vrij kostbare, maar nog een redelijk onbekende maatregel vormt de zogenaamde Virtual Research Workspace ("VRW"). De VRW levert een beveiligde en afgeschermde omgeving met meerdere maatregelen om risico's binnen het onderzoek te kunnen mitigeren. De VRW is geen omgeving waar op centraal niveau regie op plaatsvindt. De ontwikkeling en ondersteuning is zeer afhankelijk van enkele personen bij het DCC en CIT.

Aanbeveling

- Formuleer een duidelijke en onderbouwde visie op de inrichting van informatiebeveiliging en neem dit mee bij het implementeren van eigenaarschap, zoals beschreven in hoofdstuk 1.
- Ondersteuning voor onderzoekers blijft noodzakelijk op het gebied van informatiebeveiliging, zowel in middelen als in kennis. Neem de regie op enkele organisatiebrede maatregelen, zoals het Research data management system en draag zorg voor doorontwikkeling.

8 Informatieverstrekking en rechten betrokkenen

De Rijksuniversiteit Groningen dient transparant te zijn over de verwerking van persoonsgegevens van studenten, medewerkers en onderzoeksdeelnemers. Niet alleen omdat dit wettelijk vereist is, maar ook om het vertrouwen in de instelling te bevorderen. Met het volwassener worden van de organisatie, groeit ook de mate van transparantie, wat een positieve ontwikkeling is. Bij tal van verwerkingen worden studenten en medewerkers geïnformeerd, hoewel vaak nog volstaan wordt met een verwijzing naar de meer algemene (organisatiebrede) privacyverklaring. Deze privacyverklaring is goed geformuleerd, maar te algemeen om te voldoen aan de eisen voor een specifieke verwerking. In de bedrijfsvoering en het onderwijs zou men kunnen leren van het wetenschappelijk onderzoek, waar vaak een specifieke en heldere privacyverklaring of informatiebrief wordt verstrekt aan de betrokkenen (onderzoeksdeelnemers).

Transparantie en het gepubliceerde register

Een positieve ontwikkeling is het groeiende overzicht met verwerkingen in het register dat inzichtelijk maakt welke gegevens waar worden verwerkt en waarom. Het is echter van belang om als betrokkene inzicht te hebben in de details van de verwerking op het moment dat de RUG haar/zijn persoonsgegevens verzamelt of op het punt staat deze te gaan verwerken. Het tonen van de desbetreffende beschrijving uit het register op het juiste moment en op de juiste plaats vormt derhalve nog een mooie kans. Bij de opzet of introductie van nieuwe verwerkingen kan dit ook worden meegenomen.

Naast het verschaffen van inzicht in de wijze van verwerking, hebben betrokkenen ook de gelegenheid om (beperkt) wijzigingen aan te brengen in hun persoonsgegevens. Dit kan middels een aantal centrale gebruikersportalen (o.a. Progress en AFAS), of door de RUG te contacteren via

privacy@rug.nl. Het overgrote gedeelte[18] van verzoeken van betrokkenen wordt op tijd behandeld en beantwoord. De manier waarop betrokkenen bij de RUG gebruik kunnen maken van hun wettelijke rechten is een solide proces en wekt het gewenste vertrouwen.

9 Verwerkers en doorgifte

Er werken talloze organisaties in opdracht van de RUG met persoonsgegevens, ook wel “verwerkers” genoemd. Naast de verantwoordelijkheid van de universiteit voor deze gegevens, dragen deze verwerkers ook de verantwoordelijkheid om passende beschermingsmaatregelen te nemen, zelfs (of met name) wanneer zij zich buiten de Europese Economische Ruimte (EER[19]) bevinden. Het effectief controleren van deze maatregelen is complex en kostbaar, en vormt een uitdaging voor de RUG.

Onderzoek en onderwijs over de grenzen

Binnen de faculteiten en diensten worden vaak (internationale) afspraken gemaakt die niet altijd in lijn zijn met de richtlijnen van de RUG voor gegevensdeling. Desalniettemin is het delen van gegevens cruciaal voor regionale, nationale en internationale samenwerking op het gebied van onderwijs en onderzoek. Het is bij onderzoek daarom van belang om onderzoekers in een vroeg stadium te informeren en te adviseren. Adequate onderzoeksondersteuning is daarbij onmisbaar in alle faculteiten.

Binnen het wetenschappelijk onderzoek zijn er diverse stadia waarin de overdracht van gegevens opgemerkt kan worden door de onderzoeksondersteuning en vervolgens in lijn met de wet- en regelgeving kan worden gebracht. Dit omvat onder andere de fasen van het opstellen van een datamanagementplan, de ethische beoordeling en de financiële verantwoording, met name bij onderzoekssubsidie.

Binnen het domein onderzoek heerst onzekerheid over de overdracht van (persoons)gegevens buiten de EER. Ook de verantwoordelijkheden van onderzoekers in deze context zijn evenmin altijd helder. Het DCC kan hierbij ondersteuning bieden, mits het voldoende bekendheid geniet en tijdig wordt geraadpleegd.

Beleid over internationale gegevensdeling

Voor alle processen binnen de RUG geldt dat het nauwkeurig in kaart brengen van verwerkingen buiten de EER essentieel is. Het registratieproces in het register kan hierbij helpen, maar er ontbreekt beleid omtrent deze doorgifte van gegevens. Dit geldt dus niet alleen voor wetenschappelijk onderzoek, maar ook voor bedrijfsvoering, zoals bij de marketingactiviteiten op platforms als TikTok, Instagram en X. Uitdagingen rond gegevensoverdracht en het ontbreken van formeel beleid vormen obstakels voor het inzetten van verwerkers en staan centraal in discussies over het gebruik van leveranciers uit de o.a. de Verenigde Staten en China.

Ondanks het ontbreken van duidelijke beleidslijnen, zijn veel doorgiftes die door de P&S-coördinatoren of het centrale privacyteam worden opgemerkt, geregistreerd en nageleefd conform de wet- en regelgeving. Dat gebeurt bijvoorbeeld door het maken van (internationale) afspraken in de verwerkersovereenkomst, maar ook het uitvoeren van een risico-inventarisatie (DPIA) voor het land van de ontvangende partij.

[18] Met de tijdelijke afwezigheid van een P&S-coördinator bij de studentenadministratie kon de RUG niet tijdig voorzien in de beantwoording van vijf verwijderverzoeken en één inzageverzoek.
[19] De EER bestaat uit de Europese Unie plus IJsland, Liechtenstein en Noorwegen.

Stel duidelijke richtlijnen op voor het delen van gegevens met partijen buiten de EER en waarborg dit proces adequaat. Zorg er daarbij voor dat deze richtlijnen in overeenstemming zijn met de sectorale richtlijnen, zoals die van SURF.

Aanbeveling

10 Datalekken

De manier waarop incidenten en datalekken worden afgehandeld is het afgelopen jaar gewijzigd. De CPO is benoemd tot de regisseur van dit proces. Daarbij is de beweging ingezet om de behandeling van laagrisico-datalekken toe te wijzen aan de P&S-coördinatoren. Met de groei van de professionaliteit en kennis van de P&S-coördinatoren, is dat een logische stap. Zij kunnen als geen ander de impact op mensen en de (decentrale) organisatie inschatten. Ook de gevolgde trainingen (zie hoofdstuk 2) dragen hieraan bij.

Een wenselijke vervolgstap ziet op het verder implementeren van indicatoren waarop het CvB en/of de CPO kan bijsturen in het datalekkenproces. Hierbij kan gedacht worden aan het sturen op maatregelen, zoals beveiligd delen van gegevens, wanneer er veel datalekken met de reguliere (onbeveiligde) e-mail zijn. Een helder overzicht van het type incidenten is daarvoor belangrijk, en daarom is besloten om het incidentenbeheer onder te brengen in TopDesk.

Positieve ontwikkeling - meer gemelde incidenten

Het aantal gemelde incidenten (**59**) is sterk gestegen ten opzichte van het voorgaande jaar (28). Van die incidenten zijn **40** daadwerkelijk als datalek gekwalificeerd. De meerderheid daarvan betrof een datalek met een laag risico voor de betrokkenen en de universiteit. Voorbeelden hiervan zijn 1) een e-mailen met niet-gevoelige inhoud naar de verkeerde persoon en 2) het achterblijven van gegevens op een uitleenlaptop. Er zijn **twee** datalekken met een hoog risico aangemerkt; deze zijn gemeld bij de Autoriteit Persoonsgegevens.
Het is goed te vermelden dat de stijging van het aantal datalekken bijzonder genoeg een hoopgevende oorzaak heeft; medewerkers herkennen een incident eerder én de bereidwilligheid om te melden is groter. De RUG is ondanks een hoger aantal gemelde incidenten, dus niet aantoonbaar onveiliger of onzorgvuldiger met gegevens omgegaan.

Zorg ervoor dat de voorgestelde maatregelen grondig worden opgevolgd om het aantal toekomstige datalekken te beperken. Hierbij kan een Incident Management Systeem helpen en is het belangrijk om te blijven analyseren wat de oorzaken van incidenten zijn.

Aanbeveling

Vooruit(kijken)

In het eerste kwartaal van 2024 komt het Programma tot een einde en worden taken en verantwoordelijkheden overgenomen door de staande organisatie. Vooralsnog lijkt dit geen eenvoudige overgang. Waar het Programma een specifieke focus en middelen heeft, hebben faculteiten en diensten dat niet altijd. Om het huidige momentum vast te houden wordt er van het CvB gevraagd scherp te zijn op opvolging van de binnen het Programma besloten thema's. Ook in de te voeren bestuursoverleggen ("BO's") is het verstandig specifiek aandacht aan de Werkplannen en de onderliggende PDCA-cylci van diensten en faculteiten te besteden, zodat waar nodig kan worden bijgestuurd óf gecomplimenteerd.

De uitdagingen binnen de RUG blijven liggen op het verder beschrijven en toepassen van het eigenaarschap, maar ook het inrichten van gegevensbescherming binnen de bestaande onderzoeks(ondersteunings)processen. Hierbij wordt meer aandacht en initiatief van de decanen gevraagd om onderzoek in kaart te brengen, maar ook om (decentrale) *best practices* te ontwikkelen, toe te passen en intern te delen. Zoals vorig jaar en eerder in dit verslag beschreven is, kan het DCC hierbij helpen.

Met de afronding van het Programma tonen de cijfers 'slechts' een lichte groei in de volwassenheid. Echter, achter de cijfers schuilt een forse groei in kennis en vaardigheden van alle betrokken medewerkers, wat gepaard gaat met een waarneembare verandering in de organisatiecultuur. Deze ontwikkelingen zijn zichtbaar op alle niveaus binnen de RUG. Ook zijn verantwoordelijkheden verhelderd, en groeit het besef van de noodzaak om zorgvuldig met mensen en dus persoonsgegevens om te gaan. Al met al een positief beeld voor een diverse, complexe en internationaal georiënteerde organisatie.

Slotwoord functionaris gegevensbescherming

Met mijn aankomend vertrek in maart, is dit ook het laatste jaarverslag bescherming persoonsgegevens dat ik schrijf voor de Rijksuniversiteit Groningen als FG. Daarmee sluit ik een werkzame periode van zeven jaar af bij de universiteit. In die zeven jaar is de universiteit enorm gegroeid op het thema gegevensbescherming. Dit is te danken aan, in de eerste plaats de P&S-coördinatoren en de privacyjuristen/CPO, maar was (financieel en organisatorisch) onmogelijk geweest zonder de welwillendheid van het College van Bestuur en faculteitsbestuurders.

De ontwikkeling van de privacymanagementorganisatie is zeer afhankelijk geweest van de bijzondere kenmerken van deze organisatie. De organisatie kenmerkt zich door het hoge niveau waarop medewerkers hun werkzaamheden willen doen en een enorme *drive* om dat te bereiken. Dit maakt ook dat de snelle (organisatorische) ontwikkelingen soms wrijving veroorzaken; financieel, dan wel organisatorisch. Een bekende kreet binnen de instelling is echter ook "zonder wrijving geen glans".

Naast het hoge niveau en het doorzettingsvermogen kenmerkt deze organisatie zich natuurlijk door het multidisciplinair onderzoek/onderwijs en een grote focus op regionale samenwerking met een uitgebreid internationaal netwerk. Om die reden waren de "connections" binnen de organisatie tussen de verschillende groepen (gegevensbeschermingsprofessionals, securityspecialisten, WP en OBP) onmisbaar om verder te komen.

De Rijksuniversiteit Groningen mag trots zijn op haar mensen en hetgeen op dit thema bereikt is.

Bij deze wil ik alle collega's bedanken voor de mooie samenwerking. Ik heb enorm veel geleerd en genoten van het werk en het contact. De universiteit verlaat ik, maar Groningen niet, want er gaat niets boven Groningen.