rijksuniversiteit groningen

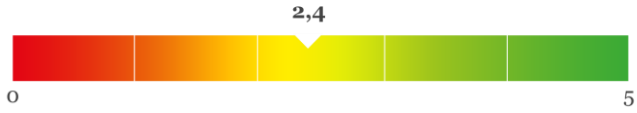
Jaarverslag bescherming persoonsgegevens 2022

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 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. In 2021 is de RUG gestart met verscheidene beheerprocessen. In 2022 is een deel geïmplementeerd en zijn er maatregelen genomen naar aanleiding van het Programma Veilig en Vertrouwd ("Programma"). Beide bewegingen resulteerden in een zichtbare groei van de volwassenheid van de RUG, met een gemiddeld niveau van **2,4**.[1]



De RUG heeft 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.

1 Privacybeleid en inbedding in de organisatie

Er tekent zich een verbeterd samenspel af tussen *de faculteiten* enerzijds en *diensten* en *CvB anderzijds* wanneer het gegevensbescherming (in de volksmond "privacy") betreft.
Beleid(sbeslissingen) word(t)(en) vaker organisatiebreed afgestemd, wat leidt tot meer duidelijkheid voor medewerkers en studenten. Privacy- en securitycoördinatoren binnen de faculteiten/diensten worden daarnaast beter gevonden, maar behoeven meer training en opleiding.
Wegens het lopende Programma zijn alle faculteiten en diensten afgelopen jaar niet om een werkplan, maar enkel om een evaluatie van het voorgaande werkplan gevraagd; deze zijn aangeleverd en centraal beoordeeld.[2] In 2023 wordt de reguliere PDCA-cyclus met Werkplannen hervat.
Het Programma heeft verder in 2022 meerdere Business Impact Assessments ("BIA's") uitgevoerd met een focus op gegevensbescherming en informatiebeveiliging. Aan de hand van de BIA's zijn risico's en behoeftes geïdentificeerd. Hierover meer in paragraaf *2 Risicomanagement*.

Aanbeveling

- Belangrijk aandachtspunt voor de RUG blijft de kennisontwikkeling in de eerste en tweede lijn; zowel mensen op de werkvloer, als privacy- en securitycoördinatoren, als managers hebben voldoende kennis nodig om privacy te borgen en te adresseren in de organisatie.
- Verder vraagt de inrichting en positionering van de P&S-organisatie een besluitvaardig CvB, nu er meerdere voorstellen liggen.

[1] In 2021 werd bij de RUG nog een volwassenheidsniveau van 2,1 vastgesteld. 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

Naast beleid en de PDCA-cyclus vormt risicomanagement een onmisbare pijler voor gegevensbescherming. Risicomanagement betekent: 1) weten wie welke gegevens verwerkt; 2) welke risico's daarbij horen; en 3) het formuleren en toepassen van maatregelen. Het begint echter met het duidelijk formuleren van (interne) verantwoordelijken; een duidelijk aandachtspunt voor de universiteit.

Om risicomanagement naar een hoger niveau te tillen, juicht de FG de voorgestelde "proces- en risicomanagementrollen" van het Programma toe. Hierbij wordt verhelderd wie eigenaar is voor welk(e) proces, risico, systeem en data. De P&S-organisatie[3] is op haar beurt ondersteunend aan deze eigenaren. Het is van belang dat alle medewerkers zorgvuldig omgaan met (persoons)gegevens, dit is géén exclusieve taak van P&S-coördinatoren, wat weleens zo wordt gezien.

Naast de governance vraagt het toewerken naar een organisatiebrede risicomanagementaanpak om bewustwording van de eigen rol op de werkvloer. Het integraal opnemen van risicomanagement binnen de Werkplannen is een stap in de goede richting. Hierbij wordt aansluiting gezocht bij het cyclisch proces waarmee het register (van verwerkingen) wordt gevuld.
Daarnaast is de RUG nog zoekende hoe het risico-inventarisaties (DPIA's), en Privacy by Design structureel toegepast krijgt bij nieuwe verwerkingen. Dit vraagt om deelname van alle stakeholders en derhalve de hele keten bij ontwikkeling en implementatie van nieuwe processen. Vanuit het perspectief van gegevensbescherming is dit suboptimaal verlopen bij Brightspace en Mobile Device Management. Hier komt een hiaat om de hoek kijken die in paragraaf *6 Bewaren van persoonsgegevens en opslagbeperking* verder wordt toegelicht en ziet op een breder thema: informatiemanagement.

Daarentegen toont het DPIA op Cynet (End Point Protection) en meerdere DPIA's op voorgenomen wetenschappelijke onderzoeken dat in de lijn steeds vaker aan risicomanagement wordt gedaan. Verder kan het uitvoeren van een DPIA resulteren in kennisvergroting bij deelnemers en wordt daarmee "Privacy by Design"-werken ook meegenomen in de reguliere processen.

Aanbeveling

- Begin bij het begin, draag zorg voor risicomanagement bij het opzetten van nieuwe processen en systemen. Het RIO[4] vormde een 'best practice' en nam als onafhankelijk orgaan binnen de RUG de informatiebeveiliging, gegevensbescherming en archivering mee bij vraagbundeling, -articulatie en de opzet van aanbestedingen.
- Zorg voor periodieke training van projectmanagers op het gebied van gegevensbescherming, meer specifiek de inzet van een DPIA.

[3] Hieronder vallen onder meer de privacy- en securitycoördinatoren, Chief Privacy Officer ("CPO"), Chief Information Security Officer ("CISO"), privacyjuristen en Information Security Officers.
[4] Het RUG Information Office en de Architectuurraad zijn in 2021 tegen het advies van de IT-auditor en FG opgeheven en opgegaan in het CIT.

3 Kwaliteitsmanagement

Bij kwaliteitsmanagement hebben we het over processen om zorg te dragen voor correcte, betrouwbare en volledige data. En niet te vergeten het actueel houden van gegevens.
Zonder kwaliteitsmanagement leidt wetenschappelijk onderzoek tot de verkeerde of ongewenste resultaten. Medewerkers ervaren een slechte dienstverlening of worden benadeeld, denk aan een bevestigingsbrief van de eigen ziekmelding die op het verkeerde adres wordt bezorgd.[5] Of het magazine “Broerstraat 5” dat *en masse* naar de verkeerde adressen wordt verzonden, omdat de adresgegevens niet actueel en daarmee incorrect kunnen zijn.[6]

Binnen de RUG is een onderscheid zichtbaar in de processen per domein. Bij wetenschappelijk onderzoek, waar datamanagementplannen worden gehanteerd, vormt datakwaliteit een onmisbaar aspect van het onderzoek. Daarentegen is binnen de bedrijfsvoering de datakwaliteit een minder grote prioriteit. De onbekendheid met verantwoordelijkheden, zoals beschreven in paragraaf *2 Risicomanagement*, maakt dat afdelingen/medewerkers zich onterecht hier niet verantwoordelijk voor voelen en het borgen van datakwaliteit geen prioriteit heeft.

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

De datakwaliteit, ook wel “juistheid van persoonsgegevens” vraagt om duidelijke verantwoordelijkheden en focus bij het opzetten van (nieuwe) processen. Borging van datakwaliteit is onder meer een vast onderdeel van het DPIA-format van de RUG. Ook het toegankelijk maken van gegevens voor betrokkenen (de medewerkers, studenten, alumni en onderzoeksdeelnemers) helpt enorm bij het actueel en correct houden van gegevens.

4 Register

Inzicht hebben in de processen met persoonsgegevens. Dat gebeurt aan de hand van het register. Sinds 2022 is het register van de Rijksuniversiteit Groningen operationeel én online gepubliceerd. Voor de beschrijving van de processen zijn de faculteiten en diensten verantwoordelijk. Op centraal niveau worden deze verwerkingen beoordeeld op de beginselen uit de AVG, zoals dataminimalisatie, rechtmatigheid, doorgifte, etc.
Publicatie van het register vormt een mijlpaal; de toegevoegde waarde zit in de transparantie die hiermee gecreëerd wordt, maar nog belangrijker is de inrichting van de beheerprocessen waarbij processen tegen het licht worden gehouden. Een goed functionerend register gaat de universiteit helpen bij het efficiënter en zorgvuldiger inrichten van onderwijs- en bedrijfsprocessen. Ook kan er met behulp van het register gestuurd worden op risico’s, omdat de inhoud en werking van processen duidelijk wordt.

Binnen het domein onderzoek ontbreekt nog altijd centrale aansturing en een concrete start bij veel faculteiten om grip te krijgen op de verwerking van persoonsgegevens. Het verkrijgen van inzicht en overzicht blijft dan ook een uitdaging. Een oplossingsrichting die aansluit bij het datamanagementbeleid en helderheid schept over de gedeelde verantwoordelijkheden heeft de voorkeur. In het verlengde hiervan is het effectief om disciplinespecifieke onderzoeksscenario’s te

[5] Dit is een incident dat voorgevallen is in 2022.

[6] Studentenhuizen ontvangen grote aantallen van het magazine *Broerstraat 5*, omdat de RUG niet beschikt over een juist en actueel adres van (voormalige) studenten die daar hebben gewoond.

beschrijven met de daarbij behorende maatregelen. Dit scheelt de onderzoeker veel werk en draagt bij aan een gestructureerde en verantwoorde verwerking van persoonsgegevens in wetenschappelijk onderzoek. Ook vraagstukken omtrent *open science* en de *FAIR-principes* zijn onderdeel van deze scenario's.

- Om beter te kunnen sturen op het mitigeren van de (hoogste) risico's doet de RUG er goed aan om alle diensten en faculteiten hun processen zoveel mogelijk te laten invullen in het register. Dit leidt tot een meer verantwoorde wijze van omgaan met data.
- Voor het wetenschappelijk onderzoek is het gewenst om toe te werken naar een uniforme wijze van registratie waarbij onderzoeksscenario's worden gehanteerd. De, in ontwikkeling zijnde, UniRequest van de faculteit GMW vormt een eerste stap, maar centrale regie/ondersteuning bij de opzet en uitrol hiervan ontbreekt.

Aanbeveling

5 Doelbinding en intern toezicht

Binnen *gegevensbescherming* is "doelbinding" een fundamenteel principe. Het vereist dat persoonsgegevens enkel worden gebruikt voor het specifieke doel waarvoor ze initieel zijn verzameld.

Het borgen van doelbinding is een uitdaging. Schending ervan ligt op de loer, zoals bij het voorgenomen gebruik van IP-/MAC-adressen van apparaten van medewerkers tijdens de coronacrisis. Hierbij zouden de adressen, geregistreerd door internetrouters, ingezet worden voor controle op de aanwezigheid van medewerkers.[7] De praktijk toont dat faculteiten en diensten de doelen nog veelal informeel bepalen en uniformiteit nog niet wordt nagestreefd. Vergelijkbare verwerkingen binnen faculteiten hebben uiteenlopende doelen. Daarbovenop wijkt de informatie richting studenten en medewerkers af van de initiële doelen.

Met de implementatie van het register is wel een beheerproces ingericht. Dit betekent simpelweg dat er (toe)zicht is op de verwerkingen van persoonsgegevens en er onder meer gestuurd kan worden op doelen, bewaartermijnen en dataminimalisatie. Het geeft de FG tegelijk handvatten voor beter toezicht op een risicogebaseerde wijze.
Ook is het uniformeren van gewenste verwerkingen binnen onderwijs en bedrijfsvoering nu haalbaar. Daarbij kunnen *best practices* uit de branche als uitgangspunt worden genomen. Om te zorgen voor verbetering en uniformiteit is een cyclisch proces van enkele jaren vereist.

Om tot een effectieve controle te komen op de doelen van verwerkingen van persoonsgegevens, is het van belang om zo veel mogelijk doelen en gestandaardiseerde processen op organisatiebrede wijze vast te stellen. Doelen dienen daarbij te worden gekoppeld aan deze standaardprocessen.

Aanbeveling

Toezicht en positionering FG

De FG voert binnen de RUG zijn werk onafhankelijk uit. Dit is organisatorisch geborgd. Hieronder valt een rechtstreekse communicatielijn met de leden van het CvB en zitting in de Strategische Commissie

[7] Op de "Aanwezigheidsregistratie" is een DPIA uitgevoerd waaruit bleek dat het gebruik van herleidbare "wifi-gegevens" onrechtmatig was.

Privacy en Security (“commissie”). De commissie bestaat uit: een lid van het CvB en vertegenwoordiging van de faculteitsbestuurders en directies, en overlegt elk kwartaal.

In 2022 hebben ook structureel overleggen plaatsgevonden tussen de FG en de CPO en de CISO. Ook sprak de FG eenmaal met de leden van de Raad van Toezicht en meerdere malen met U-raadsleden.

Verder heeft de FG het CvB eind 2022 verzocht om structurele secretariële ondersteuning, onafhankelijk van de middelen van ABJZ, om zijn werk naar behoren te kunnen blijven uitvoeren. Er is nog geen beslissing genomen over dit verzoek.

Met de doorontwikkeling en publicatie van het register heeft de FG meer inzicht in de verwerkingen gekregen en dat aangegrepen om inhoudelijk meer met de P&S-coördinatoren te spreken.

Als laatste is de FG, in samenwerking met de IT-auditor, een audit gestart op Brightspace. Wegens een moeizame samenwerking met de betrokken diensten was de voortgang in 2022 beperkt en is de audit nog niet afgerond ten tijde van schrijven van dit verslag (6 april 2023).

6 Bewaren van persoonsgegevens en opslagbeperking

Aansluiten bij de bewaartermijnen in de branche, en daarmee het volgen van de zogenaamde *Selectielijst Universiteiten en Universitaire Medische Centra*, is een vrij onbekende plicht van de RUG. Het is daarom niet verrassend dat het gecontroleerd archiveren en verwijderen van gegevens bij de universiteit amper is ingericht, al worden sinds kort ‘opruimacties’ georganiseerd.

Samengevat worden gegevens langer bewaard dan nodig en worden gegevens die wel bewaard of gearchiveerd moeten worden, niet op de juiste wijze behandeld. Opslag vindt versplinterd plaats over tal van gegevensdragers, waardoor de samenhang ontbreekt en het heel moeilijk wordt, zo niet onmogelijk, om informatie uit afgeronde werkprocessen te reconstrueren. Dit speelt binnen alle domeinen. Zo kennen Brightspace en AFAS geen procedures om archiefplichtige documenten eruit te halen. Hierdoor ontbreekt grip op de vereiste administratieve neerslag.

Brightspace, AFAS en ook Progress.NET, zijn geïmplementeerd als zogenaamde “stapelapplicaties” waarin we gegevens vanaf het moment van ingebruikname blijven opslaan, maar niet ordenen, van voldoende kenmerken voorzien, archiveren of vernietigen. Dit heeft aanzienlijke kosten en tijdverlies tot gevolg voor de universiteit, zoals de opslag van overbodige data én de tijd die nodig is om gegevens op het juiste moment binnen processen te kunnen inzetten. De gehanteerde werkwijze is te vergelijken met een pakhuis zonder inventarislijst.

Uiteindelijk gaat het om meer dan enkel opslaan, verwerken en archiveren/verwijderen van gegevens. Het gaat hier om informatiemanagement. Binnen de RUG is beperkte regie op informatiemanagement, dat wil zeggen de logische samenhang tussen informatiestromen, bedrijfsprocessen en organisatiedoelen. Vanaf het moment van binnenkomen van digitale bedrijfsinformatie, in applicaties of e-mailboxen, of het ontstaan van informatie binnen de muren van de RUG ontbreekt centrale regie en beleid over hoe al deze informatie te geleiden en de onderlinge samenhang te bewaken. Dit is een breder vraagstuk dat de taken van de IT-leverancier (CIT), de afdeling Documentaire Informatievoorziening (DIV) of ABJZ overstijgt. Informatie-management vereist een overkoepelende sturing en kennis van informatiearchitectuur binnen de hele RUG. Helaas is hierover in de afgelopen drie jaren veel kennis en expertise verloren gegaan.

Een positieve noot is wel de start binnen de verschillende faculteiten van het begeleiden van veel (centrale) bestuursprocessen en bijvoorbeeld van de digitalisering van de postkamer. Het betreft de eerste stap en vereist daarom nog uitbreiding en verbetering.

Een ander aandachtspunt is het duurzaam opslaan en verwijderen van gegevens in communicatiemiddelen als e-mail en berichtenapps. Dit proces is nog niet gestart en binnen de RUG zijn er nog geen stappen ondernomen om dit op te zetten. Als gevolg hiervan gaat veel cruciale informatie verloren.

- Om bewaartermijnen in het onderzoek vast te stellen, wordt aangeraden om aansluiting te zoeken bij de landelijke netwerken en disciplinespecifieke richtlijnen.
- Zet organisatiebreed in op de professionele inrichting van informatiemanagement. Gezien het faculteit-/dienstoverstijgende karakter, dient initiatie vanuit het CvB te komen.

Aanbeveling

7 Beveiligen van persoonsgegevens

Gegevensbescherming is vrijwel niet mogelijk zonder informatiebeveiliging. De faculteiten en diensten zijn in beginsel verantwoordelijk voor de toepassing ervan. Binnen de RUG heerst er verwarring over informatiebeveiliging. Informatiebeveiliging wordt onterecht gelijkgesteld aan ICT-beveiliging. Dit voorkomt echter een effectieve aanpak en leidt tot vingerwijzen richting het CIT.

Deloitte heeft in het kader van het Programma een inventarisatie uitgevoerd op het volwassenheidsniveau van de organisatie ten aanzien van informatiebeveiliging. De inventarisatie toont aan dat informatiebeveiliging nog een lage volwassenheid heeft. Daarbij helpt niet mee dat het centrale securityteam klein is en de inzet van externen maakt de borging van kennis over de organisatie moeilijker. Ook speelt het gehele jaar de discussie omtrent de positionering van de CISO en daarbij het team van de Information Security Officers (“ISO’s”). De discussie loopt lang en heeft nog weinig toegevoegde waarde opgeleverd voor de organisatie van informatiebeveiliging.

Naast het opschorten van interne opleidingsmogelijkheden voor P&S-coördinatoren, heeft een tekort aan ISO’s niet bijgedragen aan het opleiden van de P&S-coördinatoren op het thema informatiebeveiliging.

Binnen het wetenschappelijk onderzoek is vraag naar passende technische en organisatorisch maatregelen om onderzoek (met gevoelige data) te kunnen uitvoeren. Het DCC biedt hierin beperkte ondersteuning, maar groeit wel in de (ondersteunings)rol. Daarnaast kan de Virtual Research Workspace (“VRW”) uitkomst bieden mits afdoende beheer en doorontwikkeling plaatsvindt.

- Werk toe naar een onafhankelijk gepositioneerde CISO die verantwoording aflegt aan het CvB en gesprekspartner is van de diensten met gevoelige data (zoals AMD, HR en SIA), maar niet beschouwd wordt als een CIT-onderdeel.
- Het is van belang om P&S-coördinatoren de basiskennis bij te brengen over informatiebeveiliging.
- Daarnaast is ondersteuning voor onderzoekers noodzakelijk op het gebied van informatiebeveiliging, zowel in middelen als in kennis. Hierbij kan het DCC een belangrijke rol spelen. Hoewel initiatieven zoals de VRW belangrijk zijn, bieden ze momenteel nog een te beperkte dienstverlening aan onderzoekers.

Aanbeveling

8 Informatieverstrekking en rechten betrokkenen

De RUG moet transparant zijn over het gebruik van persoonsgegevens van studenten, medewerkers en onderzoeksdeelnemers. Dit draagt bij aan het vertrouwen in de instelling. Met de volwassenheidsgroei van de RUG wordt ook de transparantie groter; een positieve ontwikkeling. Het register draagt hier sterk aan bij (zie paragraaf *4. Register*).

Verbeterpunten zijn met name te behalen bij de introductie van nieuwe processen/applicaties. Een voorbeeld: studenten kunnen duidelijker geïnformeerd worden over de verwerking van hun gegevens in de leeromgeving (Brightspace). Docenten kunnen per individuele student inzien welk document geopend is en hoe laat hij/zij voor het laatst in de leeromgeving heeft ingelogd. Los van de (on)wenselijkheid van een dergelijke verwerking en mogelijke schending van dataminimalisatie, hebben de meeste studenten geen weet van een dergelijke verwerking. Des te vervelender is het wanneer een docent een student aanspreekt op het al dan niet gelezen hebben van stukken op basis van die gegevens.[8]

Naast transparantie hebben betrokkenen ook de mogelijkheid om hun persoonsgegevens (beperkt) aan te passen. De wijze waarop de RUG hiermee omgaat, wekt vertrouwen en is solide uitgevoerd.

9 Verwerkers en doorgifte

Bij de verwerking van persoonsgegevens maakt de RUG gebruik van honderden organisaties, oftewel “verwerkers”. Naast de verantwoordelijkheid van de RUG, hebben verwerkers ook een verantwoordelijkheid om passende beschermingsmaatregelen te treffen, zelfs wanneer zij zich buiten de EER bevinden. De effectieve controle op deze maatregelen is ingewikkeld en kostbaar, wat een uitdaging vormt voor de RUG

Doorgifte van gegevens is noodzakelijk voor regionale, nationale en internationale samenwerking op het gebied van onderwijs en onderzoek. Binnen de faculteiten worden met grote regelmaat (internationale) afspraken gemaakt die niet in lijn zijn met de kaders die de RUG aanhoudt. Zo bestaat er bij onderzoekers nog veel onbekendheid over de doorgifte van (persoons)gegevens buiten de Europese Unie (meer specifiek: de EER[9]). Ook de (eigen) verantwoordelijkheid van de onderzoeker hierbij is niet altijd helder. Het DCC kan hierin assisteren mits het meer bekendheid geniet en tijdig wordt betrokken.

Naast doorgifte binnen wetenschappelijk onderzoek, vormen de uitdagingen rondom de doorgifte van gegevens en het ontbreken van formeel beleid over internationale doorgifte een obstakel voor de inzet van verwerkers. Deze kwestie raakt aan de kern van veel actuele discussies over het al dan niet inzetten van leveranciers uit de Verenigde Staten en China.

Aanbeveling

Formuleer een helder beleid met betrekking tot de overdracht van gegevens naar het buitenland en zorg voor borging van dit proces. Sluit hierbij aan bij de kaders van SURF.

[8] Dit betreft een feitelijke casus en heeft er mede toe geleid een assessment uit te voeren op de (onderwijs)processen die door Brightspace heen lopen.

[9] Europese Economische Ruimte: de EU met Noorwegen, IJsland en Liechtenstein.

10 Datalekken

Het aantal gemelde incidenten (**28**) is licht gedaald. Van die incidenten zijn er **18** als datalek gekwalificeerd. De meerderheid daarvan is een datalek met een laag risico voor de betrokkenen en de universiteit. Een voorbeeld hiervan is het delen van een cijferlijst waarop medestudenten worden vermeld. Er is **één** datalek gemeld bij de Autoriteit Persoonsgegevens dat later echter weer is ingetrokken.

Een logische 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, bij veel datalekken met de reguliere (onbeveiligde) e-mail.

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 analyseren wat de oorzaken van incidenten zijn.

Aanbeveling

Vooruit(kijken)

In 2022 is het Programma van start gegaan. Dit heeft gezorgd voor de start van verdere groei binnen met name de bedrijfsvoering en onderwijs. De gemeten groei is voornamelijk toe te kennen aan het opleveren van processen waar in de coronajaren aan is gewerkt. In 2023 worden naar verwachting (meer) processen en ‘producten’ opgeleverd uit het Programma. Risico’s voor het zorgvuldig opzetten van privacymanagement zijn in 2023: voldoende gespecialiseerd personeel vinden voor informatiebeveiliging, slagvaardigheid bij het CvB op RUG-brede thema’s en het onderkennen van goed datamanagement binnen wetenschappelijk onderzoek. Dit jaar draagt het Programma haar taken over aan de CPO en de CISO. Dit vraagt een duidelijke governance binnen de gehele universiteit op de thema’s gegevensbescherming en informatiebeveiliging.

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.

rijksuniversiteit groningen

Managementreactie College van Bestuur - Jaarverslag bescherming persoonsgegevens 2022

Datum	20 april 2023
Auteur	J.W. Oordt LL.M., Chief Privacy Officer ABJZ

Inleiding
Elke student, elke medewerker, elk onderzoekssubject en ieder ander moet erop kunnen vertrouwen dat zijn of haar persoonsgegevens door de Rijksuniversiteit Groningen (RUG) rechtmatig worden verwerkt en passend worden beschermd. Te allen tijde wil de RUG zorgvuldig en behoorlijk omgaan met persoonsgegevens. De RUG wil voldoen aan de Algemene Verordening Gegevensbescherming (AVG) en een consistent en hoog niveau bieden van de bescherming van de rechten en vrijheden van individuen.[1]

De RUG heeft een Functionaris voor de Gegevensbescherming (FG) die toezicht houdt op naleving van de AVG en daarover verslag uitbrengt aan het College van Bestuur. Sinds 2018, het jaar waarin de AVG van toepassing werd, heeft de FG een jaarverslag opgesteld. Het verslag bevat een overzicht van de ontwikkelingen die hebben plaatsgevonden en beschrijft het door de universiteit bereikte volwassenheidsniveau op het gebied van bescherming van persoonsgegevens. Daarvoor wordt het volwassenheidsmodel van het CIP[2] als leidraad gebruikt. Het jaarverslag bevat aanbevelingen en adviezen waarmee de RUG verdere volwassenheidsgroei kan bewerkstelligen. Het College van Bestuur is de FG dankbaar voor zijn adviezen en kritische houding.

Terugblik 2022
De RUG heeft zich ten doel gesteld op het gebied van gegevensbescherming een gemiddeld volwassenheidsniveau van minimaal 3.0 te bereiken en te behouden. Daarmee is de organisatie in control en handelt zij actief en gestructureerd, wordt de bescherming van persoonsgegevens voortdurend verbeterd en wordt voldaan aan de AVG en andere privacywetgeving. De RUG is, zo blijkt uit de verslagen van de FG, gegroeid van een privacyvolwassenheidsniveau van 1.3 per 1 januari 2019 naar een niveau van 2.4 per 1 januari 2023. In 2022 is de RUG gegroeid van een niveau van 2.1 naar 2.4. Voor de groei in 2022 zijn de volgende redenen aan te wijzen.

1. Verdere inrichting van het verwerkingenregister, dat de processen waarin persoonsgegevens worden verwerkt beschrijft. De RUG gebruikt het register voor risicomanagement en het formuleren van maatregelen. De inhoud van het register is grotendeels beschikbaar voor studenten, medewerkers en andere belanghebbenden via de publieke website van de universiteit, hetgeen zorgt voor transparantie.[3]
2. Groei in betrokkenheid en eigenaarschap bij faculteitsbesturen en directies van diensten, onder meer dankzij de inventarisaties van het programma Veilig en Vertrouwd (het “Programma”) en de daarop gebaseerde rapportages per faculteit en dienst. Het Programma heeft bovendien het informatieportaal voor medewerkers vernieuwd en een voortdurende awarenesscampagne opgestart.
3. Professionalisering van risicomanagement. Het DPIA-template is verbeterd en door het Programma is een universitair risicobeoordelingskader geïmplementeerd. Faculteiten en diensten zijn steeds beter in staat zelfstandig privacyrisicoanalyses uit te voeren.

Het College van Bestuur onderschrijft de bevindingen en aanbevelingen van de FG in diens jaarverslag over 2022. Het College van Bestuur zal, net als voorgaande jaren, het jaarverslag van de FG beschikbaar stellen aan de Raad van Toezicht en de Universiteitsraad en het verslag met deze gremia bespreken. Het stuk wordt gedeeld met de faculteiten en diensten.

---

[1] Bron: Algemeen beleid bescherming persoonsgegevens RUG.
[2] Zie: https://www.cip-overheid.nl/media/1554/20201027_privacybaseline3_3.pdf.
[3] https://www.rug.nl/about-ug/policy-and-strategy/privacy-and-security-at-the-ug/processing-register/

rijksuniversiteit groningen

Vooruitblik 2023

De RUG acteert nog niet op het gewenste volwassenheidsniveau van 3.0. Het Programma, dat als doel heeft een privacyvolwassenheid van 2.5 te bereiken, is door het College van Bestuur verlengd tot 1 januari 2024. De manager van het Programma en de Chief Privacy Officer hebben ingezet op de volgende activiteiten.

1. Training van de universitaire gemeenschap. Het aanbod van trainingen aan medewerkers en studenten is nog niet voldoende. Er komen trainingen op maat voor doelgroepen zoals de privacy- & security (P&S) coördinatoren. De universiteit stelt een medewerker aan die dit gaat organiseren. Het CvB heeft een handreiking voor onderzoekers vastgesteld die hen helpt bij het uitvoeren van een DPIA.
2. Verbetering van de PDCA-cyclus. De RUG vernieuwt het template voor het P&S-werkplan. P&S-coördinatoren gaan een opleiding op het gebied van risicomanagement volgen. Werkplannen zijn een instrument voor faculteiten en diensten om grip op risico's te krijgen. De rapportages die in het kader van het Programma zijn opgesteld, zijn input voor het werkplan.
3. Verdere uitrol van het verwerkingenregister. Soortgelijke processen worden waar mogelijk geüniformeerd. De eerste faculteiten starten met registratie van verwerkingen in het onderzoeksdomein. Het *data management plan* dat onderzoekers maken vormt hiervoor de basis, zodat de administratieve last voor hen beperkt blijft. Het privacyteam werkt hierbij samen met het Groningen Data Competence Center. Samen met de faculteit die de Research Gateway ontwikkelt, wordt een voorstel voor *governance* van deze IT-oplossing uitgewerkt.
4. Verbetering van de governance van de P&S-organisatie. De RUG formaliseert en positioneert de functies van Chief Privacy Officer, Chief Information Security Officer en P&S-coördinator. De ondersteuning van de FG wordt verbeterd. Van faculteiten en diensten die hun P&S-organisatie niet op orde hebben, wordt verbetering verlangd. P&S-coördinatoren organiseren zich in een *P&S-gilde*, dat onder meer zorgt voor standaardinrichting van gegevensverwerkingen door middel van richtlijnen.
5. Aanscherping van het software-aanvraagproces, zodat P&S-randvoorwaarden worden meegenomen en tijdig met een DPIA of risicoanalyse wordt gestart.[4] Binnen het CIT wordt de privacyorganisatie versterkt en worden projectleiders opgeleid, zodat het CIT tijdig beschermingsmaatregelen neemt bij het implementeren van nieuwe systemen.
6. Het CvB heeft een stuurgroep informatiebeheer in het leven geroepen die een voorstel zal uitbrengen om informatiebeheer bij de RUG naar huidige standaarden en wettelijke eisen in te richten. Volwassen informatiebeheer is niet alleen een voorwaarde voor het voldoen aan de AVG, maar ook aan de Wet Open Overheid en Archiefwet.
7. Legaliseren van doorgiften. Het Programma gaat aan de slag met doorgiften van persoonsgegevens naar landen buiten het geografische toepassingsgebied van de AVG. De doorgiften worden verder in kaart gebracht en er worden maatregelen genomen zodat de doorgiften op termijn voldoen aan de AVG. Waar dat niet lukt wordt een risico-exceptie aangevraagd bij het bevoegde management. Bij deze werkzaamheden is het doorgiftenkader, dat SURF momenteel ontwikkelt, richtinggevend.
8. De afhandeling van datalekken wordt vanuit CIT overgeheveld naar de Chief Privacy Officer. Er is een incident management systeem ingericht dat zorgt voor administratie en verantwoording. Ook kan de RUG daarmee beter sturen op de toepassing van maatregelen die naar aanleiding van een datalek zijn vastgesteld. Dit systeem wordt momenteel getest door de FG en de CPO en vervolgens in gebruik genomen. In de awarenesscampagnes van de RUG zal het onderwerp 'datalekken' voortdurend punt van aandacht zijn, omdat het aantal meldingen te laag is gezien de omvang van de RUG.

Bovenstaande activiteiten sluiten aan bij de bevindingen en adviezen van de FG. Ook na afloop van het Programma zal de RUG verder moeten groeien op het gebied van gegevensbescherming. Het Programma richt hiervoor in 2023 de organisatie verder in.

[4] Uiteraard is in het aanschafproces ook aandacht voor randvoorwaarden op andere gebieden, zoals aanbestedingsrechtelijke eisen en architectuurprincipes.