rijksuniversiteit groningen

Jaarverslag 2024

Functionaris Gegevensbescherming
Rijksuniversiteit Groningen



mr. E. van Schaik

Inhoudsopgave:

Voorwoord en verantwoording van de Functionaris Gegevensbescherming 3-4

1. De inrichting en borging van de Privacy & Security-organisatie binnen de Rijksuniversiteit Groningen en het privacybeleid 5-6
2. Awareness en trainingsactiviteiten 6-7
3. Eigenaarschap en risicomanagement 7-9
4. Informatie- en Documentatiemanagement in relatie tot bewaartermijnen van Persoonsgegevens 9-10
5. Registratie verwerkingen persoonsgegevens en een register voor onderzoek 10-12
6. PDCA-cyclus risico's en maatregelen zoals verwoord in de werkplannen 12-14
7. Algemene bedrijfsvoering: 14-16
   - Risico-inventarisaties door middel van DPIA's
   - Bijzonderheden rond het algemene veiligheidsbeleid
   - Meldpunt (sociale) veiligheid
8. Datalekken 16-17
9. Externe samenwerkingsverbanden 18
10. Nieuwe ontwikkelingen: 18-20
    - Artificial Intelligence (AI)
    - Maatschappelijke ontwikkelingen en mondiale veranderingen (beveiligingsdreigingen met betrekking tot data-uitwisseling)

Tot slot 20-21

Bijlagen 22-23

Voorwoord en verantwoording van de Functionaris Gegevensbescherming

De Functionaris Gegevensbescherming (FG) houdt toezicht op de naleving van de verplichtingen die de Rijksuniversiteit Groningen als verwerkingsverantwoordelijke heeft ten aanzien van de bescherming van persoonsgegevens.
Deze verplichtingen vloeien voort uit de Algemene Verordening Gegevensbescherming (AVG).
De taken van de FG omvatten onder meer:

- De verwerkingsverantwoordelijke adviseren en informeren over de verplichtingen uit hoofde van deze verordening en toezien op naleving hiervan
- Adviseren over gegevens-effectbeoordelingen (DPIA's) en toezien op de uitvoering hiervan
- Samenwerken met de Autoriteit Persoonsgegevens (AP) en optreden als contactpersoon naar de AP

De FG houdt bij de uitvoering van deze taken rekening met de aan de verwerking gebonden risico's en met de aard, omvang, context en de verwerkingsdoeleinden.

Aanbeveling
Gelet op het feit dat op grond van de verordening de universiteit verplicht is een FG aan te stellen, ligt het in de rede de toezichthoudende functie van FG ter borging op te nemen in het Beheers- en Bestuursreglement van de universiteit.
Hierin wordt vastgelegd dat de FG diens bevindingen over de verplichtingen van de universiteit die voortvloeien uit de AVG op gezette tijden aan het College van Bestuur (CvB) voorlegt.

Bevindingen

In het jaarverslag beschrijft de FG diens bevindingen over de mate waarin de Rijksuniversiteit Groningen haar verplichtingen nakomt, welke kwetsbaarheden en risico's er zijn te onderscheiden en adviseert waar mogelijke verbeteringen en passende organisatorische en technische maatregelen noodzakelijk zijn.
Het CvB stelt het privacybeleid vast en draagt zorg voor een goede governance met name door de aanstelling van de Chief Privacy Officer (CPO) en de Chief Information Security Officer (CISO).
Het op de juiste wijze navolgen van de AVG-verordening sluit aan op de kernwaarden en ambities van de universiteit: integriteit, eerlijkheid, respect, openheid, transparantie en verantwoordelijkheid.

Bij het vaststellen van de volwassenheid van de privacymanagement-organisatie is uitgegaan van het "CIP"-model (de privacy assessment tool van het Centrum Informatiebeveiliging en Privacybescherming). Het streven is om het volwassenheidsniveau 3.0 te bereiken en behouden. In het kalenderjaar 2023 is het volwassenheidsniveau vastgesteld op 2.5.

Door onvoorziene omstandigheden heeft in het huidige verslagjaar 2024 een viertal personele wisselingen bij de invulling van de functie van de FG plaatsgevonden.
Dit heeft de continuïteit van de werkzaamheden van de FG belemmerd.
Om die reden is een aan voorgaande jaren gelijkwaardige cijfermatige rapportage over de afgelopen kalenderperiode ten aanzien van de privacymanagement-organisatie niet op te stellen, omdat het noodzakelijke inzicht in de gegevens om een betrouwbare analyse te maken ontbreekt.
Daarnaast zal met ingang van dit jaar (2025) naar verwachting een ander referentiekader gebruikt gaan worden (het zogenaamde SURF-kader), dat ook door een aantal andere universiteiten wordt gehanteerd.
Ook is ten behoeve van het maken van analyses, controles en beheer van de gegevens een governance risk and compliance-proces ingericht, ondersteund door een Governance Risk and Compliance tool (Eramba, zie bijlage 2). U leest hier meer over in paragraaf 3.
Met deze procesmatige aanpak is het mogelijk om direct te acteren op risicosignalen en om onderlinge vergelijkingen te maken tussen faculteiten en diensten.
Dit alles vraagt om een andere vorm van inventarisatie en monitoring.

!

Wèl kan gesteld worden dat, op basis van de aangeleverde werkplannen door faculteiten en diensten waarin risicoanalyses zijn beschreven en de te nemen maatregelen zijn opgenomen, ten opzichte van het kalenderjaar 2023 **een groei is waar te nemen** op het gebied van met name:

- De mate waarin risico's in kaart zijn gebracht en er maatregelen zijn genomen
- Awareness onder medewerkers
- De structuur van de Privacy & Security-organisatie.

In dit jaarverslag worden de actielijnen die zijn uitgezet naar aanleiding van de bevindingen en aanbevelingen van de FG in het jaarverslag 2023 onder de loep genomen.
Ook wordt ingegaan op een aantal aspecten van privacybeleid en risicomanagement bij de domeinen bedrijfsvoering en onderzoek.

1. De inrichting van de Privacy & Security-organisatie binnen de universiteit en het privacybeleid

Met de uitrol van het Programma "Veilig en Vertrouwd" (het Programma) in 2022 en 2023 heeft de P&S-organisatie een stevige bodem gekregen.
De Privacy & Security-coördinator (P&S-coördinator), die een centrale rol speelt binnen het domein gegevensbescherming en informatiebeveiliging, is een officiële functie geworden, met duidelijk omschreven taken en verantwoordelijkheden. Vanaf 1 januari 2024 is het Programma beëindigd en dienen de werkzaamheden door de staande organisatie te worden opgepakt.
Op grond van de vastgestelde governancestructuur dienen faculteiten en diensten hun eigen ondersteuning in te richten. In het zogenaamde drie-lijns-eigenaarschapsmodel wordt gevisualiseerd wie welke verantwoordelijkheid heeft binnen de universiteit. Hierin wordt ook aangegeven waar de P&S-coördinatoren een rol kunnen spelen (zie bijlage 1).

Het bereiken en behouden van de privacydoelstellingen en het beoogde volwassenheidsniveau vergt een voortdurende inspanning, met een actieve bijdrage van met name leden van het Privacy & Security Gilde: in het Gilde zijn ruim 25 P&S-coördinatoren van de faculteiten en diensten vertegenwoordigd.
In het Gilde werken, onder coördinatie van de Chief Privacy Officer (CPO) en de Chief Information Security Officer (CISO), de P&S-coördinatoren gezamenlijk aan RUG-brede thema's, protocollen en richtlijnen, die moeten leiden tot een verdere borging van de noodzakelijke maatregelen. Door deze interfacultaire samenwerking in diverse werkgroepen en door het uitwisselen van best practices versterkt het Gilde de kennis van de P&S-coördinatoren en draagt daarmee in belangrijke mate bij aan de implementatie van het privacy- en securitybeleid en de kracht van de P&S organisatie.
Vraagstukken die bij meerdere faculteiten en diensten spelen kunnen in Gilde-verband worden aangepakt.
Een voorbeeld hiervan is het opstellen van richtlijnen voor "Veilig werken met AI".

Doordat de P&S-coördinatoren een formele functie hebben, kunnen zij op basis van hun deskundigheid en gezag zelfstandig initiatief nemen binnen faculteiten en diensten.
De P&S-coördinatoren fungeren als vraagbaak. Zij zijn het directe aanspreekpunt en de ogen en oren van de faculteiten en diensten. Medewerkers weten de weg naar de P&S-coördinatoren steeds beter te vinden.

De Chief Privacy Officer (CPO) is verantwoordelijk voor het ontwikkelen en borgen van het door het CvB vastgestelde privacybeleid, met inbegrip van richtlijnen en procedures voor het beschermen van persoonsgegevens van studenten, personeel, onderzoekssubjecten en andere individuen.

De CPO:

- Bewaakt dat de faculteiten en diensten handelen volgens het vastgestelde privacybeleid en dat de daaruit vloeiende maatregelen toegepast worden

- Adviseert de faculteiten en diensten bij het opstellen en uitvoeren van het werkplan (zie paragraaf 6)
- Geeft de P&S-coördinatoren inhoudelijke ondersteuning
- Adviseert het CvB over de adviezen van de FG zoals genoemd in de jaarrapportage en over complexe privacy-aangelegenheden
- Initieert risicoanalyses en privacy-audits en organiseert awareness programma's
- Stuurt de privacy-organisatie aan en adviseert bestuur en management
- Zorgt voor overzicht over- en sturing op de privacyrisico's die spelen binnen de universiteit

Naast de CISO vervult de CPO een belangrijke taak in de tweede lijn van het Privacy-en Security Organisatiemodel.
Door deze positionering toont het CvB verantwoordelijkheid voor het compliant zijn op het gebied van privacy en security.
Hoewel het CvB al in 2023 heeft besloten dat de CPO bij de RUG een officiële functie zou worden, is de CPO niet eerder dan met ingang van 1 april 2024 formeel benoemd; dit heeft tot vertraging van de uitrol van diens ''Privacy Roadmap'' geleid.

2. Awareness en trainingsactiviteiten

Een van de bouwstenen van een verantwoord privacy-en securitybeleid is het bewust maken van medewerkers en studenten rond het zorgvuldig omgaan met persoonsgegevens.
In 2024 zijn in dit kader de volgende initiatieven ondernomen:

- Er is een trainingsprogramma opgezet, met name gericht op bedrijfsvoering en onderzoek. Ten tijde van de cursussen nam het aantal meldingen van datalekken toe; men werd zich bewust van welke persoonsgegevens mogelijk onrechtmatig werden en worden verwerkt. Hoe tegenstrijdig dit ook mag klinken: dit is een positief effect van de trainingen! De risico's worden meer opgemerkt en er wordt direct actie op ondernomen. Mensen tonen zich in toenemende mate bereid om tekortkomingen aan te kaarten en te melden; eerder was er schroom toe te geven dat een systeem niet goed werkt of dat er fouten worden gemaakt die tot een datalek leiden.
- Voor Masterstudenten is er een e-learningprogramma beschikbaar dat zich vooral richt op bescherming van persoonsgegevens binnen onderzoek.
- Er is een campagne ''(veilig omgaan met) onderzoeksdata'' en een campagne ''Veilig werken met AI'' gestart.
- De Stuurgroep van het Programma heeft in 2023 het besluit genomen dat een e-learning-training met betrekking tot gegevensbescherming en informatiebeveiliging een verplicht onderdeel van het onboarding programma voor nieuwe medewerkers moet worden. Deze training is in het verslagjaar ontwikkeld en wordt op korte termijn beschikbaar gesteld. Hiermee wordt een belangrijke bouwsteen van privacy- en securitybewustzijn gerealiseerd.
- Onderzoekers worden op diverse wijzen geïnformeerd over de privacyaspecten van onderzoek. In paragraaf 5 wordt hier nader op ingegaan.

- Op verschillende manieren wordt gecommuniceerd over hoe veilig om te gaan met persoonsgegevens, onder andere door informatie te delen via beeldschermen en intranet, en door het verspreiden van flyers.
- Er is een awareness campagne gehouden om het onderwerp Privacy en Security universiteitsbreed onder de aandacht te brengen.

Dit alles draagt ertoe bij dat er binnen de gehele universitaire gemeenschap een algemeen bewustzijn is ontstaan over het verantwoord omgaan met persoonsgegevens en de bescherming hiervan. Sommige faculteiten bieden ook een basistraining aan voor bachelorstudenten.

Aanbeveling
Evenals dat bij nieuwe medewerkers als onderdeel van het onboarding traject wordt aangeboden, zouden ook medewerkers die reeds in dienst zijn en alle studenten van de universiteit moeten worden verplicht een (e-learning programme) Privacy en Security te volgen.
Hierdoor ontstaat universiteitsbreed bewustzijn rond het verantwoord omgaan met persoonsgegevens.
Daarnaast blijft de aanbeveling van de FG uit het jaarverslag 2023 staan dat ook het hoger management en het CvB een training volgt op het gebied van Privacy en Security.

3. Eigenaarschap en risicomanagement

Er is nauwe samenhang tussen de vraagstukken rond eigenaarschap, dataopslag, de registratie van verwerkingen van persoonsgegevens en risicomanagement.
De risico-eigenaar is verantwoordelijk voor de primaire activiteiten van de organisatie en daarmee ook verantwoordelijk voor de eventuele risico's. De risico-eigenaar kan ook gezien worden als de 'opdrachtgever' om de processen veilig en vertrouwd in te richten. Hiertoe is het noodzakelijk dat er zicht is op wie verantwoordelijk is voor het proces van verwerken; voor het systeem waarin verwerkt wordt en wie eigenaar is van de data.
Zonder duidelijk eigenaarschap is er geen sturing mogelijk op kwaliteit en risico's.

Tevens moet worden vastgelegd waar gegevens worden opgeslagen en hoe lang de gegevens mogen worden bewaard (bewaartermijnen).
Als er geen zicht is op de dataprocessen en de verwerking van de persoonsgegevens en of- en hoe persoonsgegevens worden bijgehouden in een register, loopt de universiteit een serieus risico. De universiteit voldoet dan niet aan de verplichtingen inzake het recht op inzage, transparantie, dataminimalisatie, juistheid van gegevens en doelbinding.

Het blijkt complex om deze verantwoordelijkheden op een juiste en inzichtelijke manier te beleggen; sommige processen verlopen over meerdere organisatieonderdelen. Daarnaast wordt er gebruikgemaakt van verschillende systemen binnen hetzelfde proces. En soms zijn er meerdere eigenaren van eenzelfde proces of systeem.
Een voorbeeld hiervan is verwerking van studentgegevens in het studenteninformatiesysteem.

Ook voor het juist kunnen adresseren van risico's en te nemen maatregelen ten aanzien van privacy- en informatiebeveiliging is eigenaarschap een belangrijk uitgangspunt.
Door het juist beleggen van het eigenaarschap kunnen bijbehorende taken en verantwoordelijkheden expliciet worden gemaakt. Daarbij wordt onderscheid gemaakt in het eigenaarschap van processen, risico's, data en systemen.
Er is grote onderlinge afhankelijkheid en samenhang tussen de diverse genoemde aspecten, die onder de grotere noemer ''data information governance" te scharen zijn.

De FG heeft in het jaarverslag van 2023 een aantal opmerkingen gemaakt met betrekking tot kwaliteitsmanagement en hoe het besef van eigenaarschap hierin een rol vervult:
'*Het waarborgen van datakwaliteit, ook wel de "juistheid van persoonsgegevens" genoemd, vereist heldere verantwoordelijkheden (eigenaarschap) en aandacht bij de opzet van werkprocessen (...)'*.
Geconstateerd kan worden dat hier ten dele gehoor aan is gegeven; in 2024 is een Eigenaarschapsmodel vastgesteld. Bij het uitrollen van het Eigenaarschapsmodel zal in eerste instantie de nadruk moeten liggen op processen met de grootste risico's. Concreet zijn dit de processen rond de personeels- en studentenadministratie. De grote mate van onderlinge samenhang en afhankelijkheid van de processen maakt verwerkingen van de persoonsgegevens binnen deze sectoren risicovol. Samenwerking tussen de verschillende eigenaren en het expliciteren van de rollen leidt tot risicobeperking voor alle eigenaren.

Aanbeveling
Het CvB neemt de regie op dit onderwerp door de verantwoordelijkheid tot de uitrol en het beheer van het Eigenaarschapsmodel vast te leggen bij University Services (US).
Betrek dit model bij een bredere aanpak van data information governance.
Er is vanuit de Universiteitsbibliotheek, US en het Centrum voor Informatietechnologie (CIT) een initiatief gestart voor het inrichten van data information governance.
In aanvulling op het vastleggen van eigenaarschap moet werk gemaakt worden van het inrichten van een duidelijke governance structuur, waarbij eigenaarschap duidelijk gedefinieerd is en dat universiteitsbreed geïmplementeerd is.
Als het eigenaarschap goed is belegd, zal het volwassenheidsniveau significant toenemen, omdat er zicht is op processen en wie daar verantwoordelijk voor is, wat de risico's zijn bij de verwerking van persoonsgegevens. Daardoor zal sturing gemakkelijker worden.
Een en ander zal ook leiden tot meer efficiëntie en slagkracht.

Stel als voorwaarde bij de aanbesteding van grote informatiesystemen, zoals die van de studentenadministratie die binnenkort van start gaat, dat **privacy by design** wordt toegepast.
Daarbij wordt al tijdens de ontwikkeling van het informatiesysteem rekening gehouden met privacyaspecten, bijvoorbeeld door gedurende het proces extra (technische) maatregelen te nemen en in te bouwen om de persoonsgegevens te beschermen, zoals het vastleggen van rollen, toegangsrechten en te hanteren bewaartermijnen.

Risicomanagement

Het CvB heeft eveneens het Risicomanagementbeleid vastgesteld. Dit stelt de universiteit in staat systematisch de risico's met betrekking tot informatiebeveiliging en privacy te identificeren, beoordelen en prioriteren. Dit betreft risico's die de beschikbaarheid, integriteit of vertrouwelijkheid van informatie en persoonsgegevens kunnen bedreigen en die van toepassing zijn op alle informatie en persoonsgegevens die door of namens de universiteit verwerkt worden. Deze risico's kunnen niet alleen gevolgen hebben voor de organisatie zelf, maar ook voor de rechten en vrijheden van personen.

!

In de SURF-audit informatiebeveiliging van 2024 zijn twee risico's gedefinieerd die een directe relatie hebben met de bescherming van persoonsgegevens:

- Beveiligingsaspecten bij beheeraccounts zijn onvoldoende ingericht (niet in alle gevallen wordt gebruik gemaakt van Multi-factor Authentication) en er worden veel zogenaamde f-accounts uitgereikt die niet gekoppeld zijn aan een medewerker
- Periodieke evaluatie van toegangsrechten vindt niet of te weinig plaats

Aanbeveling
Neem de in de audit genoemde adviezen over en voer deze uit. Kort samengevat:

- Stel een formeel en gestructureerd proces op voor de evaluatie van gebruikersrechten en mutaties, inclusief periodieke controles
- Stel procedures op voor de periodieke evaluatie van toegangsrechten om onregelmatigheden te detecteren

4. Informatie- en Documentatie management in relatie tot bewaartermijnen

De universiteit is onder verschillende wetten verplicht een archief te hanteren, om informatie correct te bewaren en inzichtelijk te maken, alsook om die tijdig te verwijderen. De reikwijdte van de archiefverplichtingen is voor de universiteiten en de universitair medische centra vastgelegd in de Selectielijst Universiteiten en Universitair Medische Centra 2020.
Het betreft de neerslag van 163 werkprocessen, met hieraan verbonden bewaar- en vernietigingstermijnen.
Het onderwerp archivering en het hanteren van de juiste bewaartermijnen blijkt complex.
Het is als een veelkoppig monster: er zijn veel componenten die bepalen of data al dan niet bewaard dan wel verwijderd mogen worden en op welke termijn.
Ook is er soms sprake van botsende belangen: persoonsgegevens moeten soms op grond van de archiefverplichting langer bewaard worden dan op grond van de AVG noodzakelijk is voor het doel waarvoor de universiteit de persoonsgegevens heeft verzameld.
Dit nog los van het feit dat lang niet altijd inzichtelijk is welke data beschikbaar zijn, of deze data de juiste kwaliteit hebben, hoe en waar deze zijn opgeslagen en wie de eigenaar hiervan is.

In het verslagjaar is er binnen de universiteit op diverse wijzen aandacht besteed aan dit vraagstuk, zowel op facultair als op centraal niveau. Het werd in alle werkplannen als aandachtsveld genoemd.

Een werkgroep van Het Gilde is gestart met het verhelderen van de correcte bewaartermijnen:

- Er zijn interviews met medewerkers gehouden om het probleem in kaart te brengen
- Er is onderzoek verricht op de netwerkschijven (“y:schijf”)
- Er zijn handleidingen voor de inrichting van de y:schijven gemaakt
- Er is een lijst opgesteld van de meest gangbare termijnen
- Er is awareness gecreëerd bij medewerkers en management rond dit onderwerp

Ook worden regelmatig ‘opschoonacties’ van persoonsgegevens gehouden door de hele universiteit.
Het project rond het herinrichten van de y:schijf verloopt echter moeizaam.
Het ontbreekt de P&S- coördinatoren aan de juiste gereedschappen en middelen om dit universiteitsbreed aan te pakken. Door persoonsgegevens te lang te bewaren, of niet correct te vernietigen, overtreedt de universiteit de AVG en loopt een groter - en vooral onnodig - risico in geval van een datalek. Verschillende faculteiten en diensten hebben in hun werkplannen aangegeven een speerpunt te maken van bewaartermijnen.

!
In 2024 heeft het CvB het Volwassenheidsprogramma Informatiebeheer vastgesteld.
Hiermee is een belangrijke stap genomen in de beheersing en governance van informatiemanagement.
Dit dient in samenhang met de vraagstukken eigenaarschap, de registratie van persoonsgegevens en risicomanagement te worden bezien, zoals in bovenstaande paragrafen reeds beschreven werd. Zolang de opslagbeperking en de juistheid van de gegevens niet op orde zijn, blijft het risico dat de persoonsgegevens niet adequaat worden beschermd.
!
Als de universiteit erin slaagt deze risico's rond de verwerking van persoonsgegevens te mitigeren, zal dit een belangrijke stap zijn in het bereiken van het beoogde volwassenheidsniveau 3.

Aanbeveling
Gelet op onderlinge samenhang en afhankelijkheid, zal het Volwassenheidsprogramma Informatiebeheer onderdeel dienen uit te maken van het data information governance plan, zoals genoemd in paragraaf 3.

5. Registratie verwerkingen persoonsgegevens in het register en een register voor onderzoek

De universiteit is wettelijk verplicht een register bij te houden waarin (onder meer) wordt opgenomen welke categorieën persoonsgegevens worden verwerkt, wie verantwoordelijk is voor de gegevens en in welk systeem deze gegevens zijn opgeslagen. Met het door de universiteit

ingerichte register, dat ook publiekelijk is opengesteld, voldoet de universiteit aan de informatieplicht en de verplichting tot transparantie.
Het register is de basis voor risicomanagement; de universiteit toont hiermee haar verantwoordingsverplichting ten aanzien van betrokkenen.
Nog niet alle verwerkingen zijn in het register opgenomen. De registratie van verwerking van persoonsgegevens bij onderzoek ontbreekt vrijwel geheel. Er moet een werkproces worden ingericht dat waarborgt dat verwerkingen worden vastgelegd en waarbij de status van de verwerkingen wordt gemonitord.

Registratie van onderzoek

Binnen het domein Onderzoek neemt het Groningen Digital Competence Centre (DCC) een belangrijke plaats in. Het DCC biedt ondersteuning bij de opslag en het hergebruik van gegevens en ondersteunt de IT-infrastructuur onder meer op het gebied van onderzoeksdata- en softwaremanagement en Open Science voor onderzoekers en ondersteunend personeel.
De wijze waarop onderzoeksplannen worden ingediend en geregistreerd verschilt per faculteit. Gelet op de risico's die samenhangen met het verwerken van onderzoeksdata, verdient registratie van verwerkingen van persoonsgegevens bij wetenschappelijk onderzoek extra aandacht.
Uit de aangeleverde werkplannen en uit interviews met medewerkers van faculteiten, diensten en het DCC blijkt meermaals dat een eenduidige registratie van persoonsgegevens bij de start van een onderzoek ontbreekt. Het is niet altijd te traceren welke data worden verzameld, waar deze worden opgeslagen en hoe lang de gegevens worden bewaard.

Er lopen verschillende initiatieven naast elkaar op het gebied van de ontwikkeling van een Research Data Management Plan (RDMP) systeem.
In het verslagjaar 2024 heeft het CvB ingestemd met het voorstel om een keuzemodel voor faculteiten te ontwikkelen, waarbij zij kiezen op welke wijze zij wetenschappelijk onderzoek registreren. Faculteitsbestuurders bepalen de uitvoering vanaf 1 januari 2025 in afwachting van een RUG-breed beleid. Aan dit besluit is echter nog geen gevolg gegeven.

De faculteit GMW, die bij onderzoek de meeste persoonsgegevens verwerkt, is bezig met de ontwikkeling van een eigen registratiesysteem.
Of andere faculteiten van dit systeem gebruik willen maken is afhankelijk van verschillende factoren. Omdat het systeem nog niet operationeel is, wordt door verschillende faculteiten naar verschillende oplossingen gezocht. Coördinatie en afstemming ontbreken.
Doordat er geen deugdelijke registratie plaatsvindt, heeft de universiteit onvoldoende zicht op - en controle over de verwerking van persoonsgegevens die met onderzoek gepaard gaan en voldoet daardoor niet aan haar verantwoordingsverplichting.

Aanbeveling
Initieer een geïntegreerde aanpak door op korte termijn een universiteitsbrede Regiegroep samen te stellen waarin verschillende stakeholders vertegenwoordigd zijn.
Deze Regiegroep inventariseert de minimale eisen waaraan een RDMP-systeem moet voldoen, welk budget hiervoor noodzakelijk is, en komt, in overleg met het DCC en het College van

Decanen, tot een voorstel voor de aanschaf van een RDMP-systeem dat universiteitsbreed wordt ingevoerd.
Vertegenwoordigers van faculteiten, het cluster Research & Impact, het DCC en Bestuurlijke Juridische Zaken (BJZ) vullen de randvoorwaarden voor registratie in.
Het heeft ook vanuit oogpunt van efficiëntie voordelen vanuit één systeem te werken waarin de hele workflow van een onderzoek is opgenomen.

Studentenonderzoek binnen onderwijs

In het kader van een wetenschappelijke opleiding is het uitvoeren van onderzoek door studenten veelal onderdeel van het curriculum. Dit betekent dat een aanzienlijk aantal van de jaarlijkse studentenpopulatie onderzoeksgegevens verwerkt. Het kan hierbij ook gaan om het verwerken van persoonsgegevens. Het opstellen van een datamanagementplan is bij sommige opleidingen onderdeel van de onderzoeksscriptie. Daarbij wordt ook aandacht besteed aan het zorgvuldig omgaan met persoonsgegevens. Er is evenwel onvoldoende zicht op welke persoonsgegevens bij onderzoek worden verwerkt, waar data wordt opgeslagen en of deze weer tijdig wordt verwijderd.
Dit vraagt om duidelijke richtlijnen voor studenten over wat zij wel en niet mogen verwerken en hoelang deze data bewaard moet blijven. Daarnaast is een veilige opslagomgeving noodzakelijk waarbij de gegevens na een van tevoren vastgestelde periode automatisch worden verwijderd. Bekende applicaties als Google Drive die veelvuldig worden gebruikt zijn hier niet geschikt voor.

Aanbeveling
Stel binnen de opleidingen randvoorwaarden vast waarop studenten onderzoek mogen uitvoeren waarbij persoonsgegevens worden verwerkt en zorg voor een veilige opslagomgeving. Aandacht voor het gebruik van tools om gegevens mee te verwerken is eveneens van belang. Een en ander kan in het Onderwijs en Examenreglement (OER) worden vastgelegd.
Zoek voor de opslagmogelijkheden en voorwaarden aansluiting bij het Volwassenheidsprogramma Informatiebeheer (zoals reeds genoemd in paragraaf 4 van dit verslag).

6. PDCA-cyclus risico's en maatregelen zoals beschreven in de werkplannen

Samen met de CPO en de CISO adviseert de FG het bestuur van de universiteit over het jaarlijkse werkplan dat faculteiten en diensten opstellen voor informatiebeveiliging en privacybescherming.
In deze werkplannen wordt het privacy- en securitybeleid geëvalueerd, worden de risico's in kaart gebracht en wordt een actieplan met te nemen maatregelen opgesteld.
Hierover kan het volgende worden opgemerkt.

De faculteiten hebben de afgelopen jaren duidelijk een inhaalslag gemaakt. In vervolg op de volwassenheidsmeting die in het kader van het Programma ten aanzien van iedere faculteit en dienst is uitgevoerd en de daaraan gekoppelde risico-inventarisatie, zijn faculteiten en diensten aan de slag gegaan met het in kaart brengen van risico's, het prioriteren van te nemen organisatorische en technische maatregelen en het uitvoeren daarvan.
Een onderwerp dat in meerdere werkplannen terugkwam, was dat faculteiten meer ondersteuning van de diensten (CIT, UB, US) nodig hebben om te kunnen voldoen aan de noodzakelijke eisen die vanuit Privacy & Security worden gesteld. Verwachtingen worden niet altijd expliciet gemaakt en beschreven in een Dienstverleningsovereenkomst (DVO).

Aanbeveling
Maak expliciet afspraken over onderlinge dienstverlening met o.a. UB, CIT en US. Beschrijf hierin wat het resultaat moet zijn, wat de kosten hiervan zijn, wat de termijn van oplevering is en welke ondersteuning noodzakelijk is na oplevering. Breng in kaart wat faculteiten nodig hebben aan ondersteuning en wat de ondersteunende diensten kunnen bieden en op welke termijn. Hiermee wordt concreet of- en hoe groot er discrepantie is tussen vraag en aanbod en kan gestuurd worden op oplossingen.

De meeste faculteiten en diensten hebben een werkplan aangeleverd waaruit blijkt dat zij hun verantwoordelijkheid nemen en meer grip krijgen op hun organisatie.
Faculteiten en diensten zijn echter nog niet waar ze moeten zijn om op het beoogde volwassenheidsniveau 3 te komen.
De belangrijkste te behalen doelen waardoor risico's verder worden beperkt zijn:

- Onderzoeks(persoons)gegevens in een universiteitsbreed RDMP tool vastleggen
- Bewaartermijnen vastleggen
- Het Eigenaarschapsmodel uitrollen
- Autorisaties op juiste wijze inrichten
- Ondersteuning door CIT intensiveren

Al deze zaken moeten naast elkaar aandacht hebben. Men moet zich realiseren dat zolang een van de genoemde onderdelen nog niet voldoende op orde is, het geambieerde universiteitsbrede gemiddelde volwassenheidsniveau niet bereikt kan worden.

Nieuwe ontwikkelingen met betrekking tot de PDCA-cyclus

Zoals reeds genoemd in het voorwoord, zullen faculteiten en diensten vanaf 2025 op een andere manier hun managementactiviteiten in relatie tot privacy en security beschrijven.
Door het gebruik van het Governance Risk Compliance tool Eramba, kunnen de in kaart gebrachte risico's uitgelicht en gemonitord worden (zie bijlage 2 voor een voorbeeld).
Het systeem stelt de universiteit in staat om beveiligingsmaatregelen te koppelen aan de compliance eisen en risico's en schept een integraal overzicht over de status van de maatregelen. Doordat resultaten kunnen worden vergeleken met die van andere faculteiten en diensten wordt risicomanagement organischer en inzichtelijker en kan kennis gedeeld worden met meerdere faculteiten. Dit maakt tussentijds (bij)sturen mogelijk. Als een faculteit een oplossing heeft

gevonden of een maatregel heeft genomen om een risico te beperken, kan dat door anderen worden overgenomen. Ook hierin is de rol van het Gilde groot en wordt het belang van de inzet van P&S-coördinatoren onderstreept.

Aanbeveling
Laat alle faculteiten en diensten per 2025 verplicht werken volgens het afgesproken risicomanagementproces en laat hen gebruik maken van Eramba.
Agendeer de rapportages van de P&S-managementactiviteiten van faculteiten op de Bestuurlijke Overleggen (BO's). Het CvB blijft hierdoor periodiek in gesprek met de bestuurders over dit onderwerp, houdt hierdoor zicht op de inspanningen die zij leveren ten aanzien van de bescherming van persoonsgegevens en kan hen daar zo nodig op aanspreken.

7. Algemene bedrijfsvoering

Risico-inventarisaties door middel van DPIA's

Wanneer een bepaalde soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, waarschijnlijk een hoog risico inhoudt ten aanzien van de rechten en vrijheden van personen, dient er voorafgaand aan die verwerking een zogenaamd Data Protection Impact Assessment (DPIA) uitgevoerd te worden.
In een DPIA wordt met een divers samengesteld team wordt vanuit verschillende perspectieven in kaart gebracht:

- Welke persoonsgegevens verwerkt gaan worden
- Welke risico's geïdentificeerd kunnen worden
- Welke technische en organisatorische maatregelen geformuleerd en genomen moeten worden
- Wie de risico-eigenaar- en interne verantwoordelijken zijn.

Voordat de verwerking definitief doorgang vindt, wordt de DPIA ter advisering aan de FG voorgelegd. In 2024 zijn er 7 DPIA's uitgevoerd en van advies door de FG voorzien.
De geplande IT-audit op Bright Space, de applicatie die voor studenten binnen het onderwijs wordt gebruikt, heeft nog niet plaatsgevonden. In de applicatie zitten functionaliteiten die tegen het licht gehouden moeten worden wat betreft het voldoen aan de beginselen van de AVG.
De FG vindt het van belang dat de audit in 2025 alsnog plaatsvindt.

Het CvB is met de Universiteitsraad overeengekomen dat DPIA's die betrekking hebben op universiteitsbrede systemen waarin persoonsgegevens van studenten of medewerkers verwerkt worden, ter informatie aan de U-raad worden voorgelegd.
De U-raad kan hiermee diens recht als vertegenwoordiger van de betrokkene (de persoon op wie de persoonsgegevens betrekking hebben) uitoefenen.

Geconstateerd is dat uitvoering van een DPIA en de beoordeling van de risico's en te nemen risico beperkende maatregelen door Bestuurlijke en Juridische Zaken (BJZ) en de FG niet altijd (tijdig) plaatsvindt. In meerdere gevallen werd met de verwerking van persoonsgegevens begonnen voordat er een DPIA werd uitgevoerd of voordat een advies werd gegeven door de FG. Daarnaast is de navolging en monitoring van de risicobeperkende maatregelen, zoals in de DPIA' s vastgelegd, niet structureel belegd.
Het ligt in de rede in de DPIA de risico-eigenaar als verantwoordelijke in de DPIA vast te leggen. Dit kan in het Eigenaarschapsmodel als taak worden opgenomen.

Aanbeveling
Benadruk bij elk besluit tot gebruik van een systeem waarbij de verwerking van persoonsgegevens een hoog risico inhoudt, dat er een wettelijke verplichting is om een DPIA uit te voeren. De risico-eigenaar (vaak een faculteit of dienst) is hier verantwoordelijk voor. De P&S-coördinator kan bij de uitvoering ondersteunen.
Risicobeperkende maatregelen moeten eerst worden geïmplementeerd voordat een systeem in gebruik mag worden genomen (privacy by design).
De navolging en monitoring van de risicobeperkende maatregelen zoals in de DPIA's vastgelegd, dienen periodiek te worden geëvalueerd en als taak bij de risico-eigenaar te worden belegd.

Bijzonderheden rond het algemene veiligheidsbeleid

In het verslagjaar 2024 deed zich een aantal incidenten voor waarbij vraagstukken over privacy en security zeer actueel werden.
De universiteit werd geconfronteerd met bezettingen en met bekladding en beschadiging van het Academiegebouw en de UB.
Om de bezittingen te beschermen werd onder meer cameratoezicht ingezet. Ook waren er stewards actief bij de ingang van het pand en werden er andere beveiligingsmaatregelen genomen. Bij de keuze welke maatregelen worden ingezet moet een belangenafweging plaatsvinden tussen enerzijds het belang van de universiteit om een veilige toegang te garanderen en het gebouw te behoeden voor beschadiging en anderzijds het belang om de rechten en vrijheden van personen te beschermen. Bij cameratoezicht worden vrijwel altijd persoonsgegevens verwerkt.
Dit is slechts onder bepaalde voorwaarden en met de nodige restricties toegestaan.
Als dit toch noodzakelijk is op grond van een gerechtvaardigd belang, moeten de gevolgen hiervan zo minimaal mogelijk zijn en moeten mensen hiervan zichtbaar op de hoogte worden gesteld door middel van een (voor iedereen toegankelijke) privacyverklaring of door middel van een andere wijze van informeren. Een en ander heeft ertoe geleid dat het camerabeleid van de universiteit is geactualiseerd.

Meldpunt (sociale) veiligheid

Bij de universiteit zijn er diverse mogelijkheden om een melding of signalering te doen van een onwenselijke situatie. De universiteit draagt hiermee bij aan de zorgplicht die zij heeft ten aanzien van de universitaire gemeenschap. Deze plicht vloeit mede voort uit een aantal wettelijke verplichtingen ten aanzien van klachtenafhandeling.
Door de hoeveelheid aan loketten ontstaat het risico dat data van dezelfde persoon rond eenzelfde onderwerp op verschillende plaatsen worden verwerkt. Het is immers niet altijd duidelijk bij welk loket men precies terecht moet met de melding. Ook kan een melding of signalering meerdere componenten bevatten.
Studenten en medewerkers kunnen gebruik maken van de volgende loketten:

- Er is een meldpunt ingericht voor wetenschappers bij de universiteit die bedreigd worden of zich bedreigd voelen in de uitoefening van hun werkzaamheden (dit fungeert naast het landelijk meldpunt Wetenschap Veilig en is een gezamenlijk initiatief van UNL, KNAW en NWO)
- Er is een meldpunt wetenschappelijke integriteit als een medewerker of student een melding wil doen of een signaal afgeven over een incident rond veiligheid (in de breedste zin van het woord), kan deze terecht bij de Vertrouwenspersoon of de Ombudsfunctionaris
- Studenten kunnen voor klachten terecht bij het Centraal Loket Rechtsbescherming (CLR)
- Studenten kunnen eveneens een melding doen bij een studentendecaan.
- Studenten en medewerkers kunnen een klacht indienen bij de klachtencommissie Seksuele Intimidatie, Agressie Geweld en Discriminatie (SIAGD)
- Er is een meldpunt Sociale Veiligheid in ontwikkeling, waar studenten en medewerkers terecht kunnen die op het werk of tijdens de studie een (sociaal) onveilige situatie ervaren

Aanbeveling
Richt één centraal loket in waar alle meldingen en klachten binnenkomen.
Van daaruit kan een casemanager de melding doorzetten. Beleg de verantwoordelijkheid hiervoor bij de directie van US. Naast klantvriendelijkheid draagt dit bij aan het minimaliseren van een stroom aan (bijzondere) persoonsgegevens en daarnaast kan in sommige gevallen escalatie worden voorkomen. Het loket moet in verband met de vertrouwelijkheid met de nodige privacy en veiligheidswaarborgen worden omgeven.

8. Datalekken; aantallen, bevindingen

Bij een datalek gaat het om toegang tot persoonsgegevens zonder dat dit is toegestaan of zonder dat dit de bedoeling is en wordt veroorzaakt door een inbreuk op de beveiliging van deze gegevens. Ook het ongewenst vernietigen, verliezen, wijzigen of verstrekken van persoonsgegevens valt onder een datalek. Personen kunnen hierdoor worden geschaad in hun rechten en vrijheden.

In 2024 werden er 69 datalekken gemeld bij de FG; dit zijn er 10 meer dan in 2023.
Hiervan zijn er 4 gemeld bij de Autoriteit Persoonsgegevens; 1 daarvan werd ook bij betrokkene gemeld.
De aard van de datalekken is verschillend; in de meeste gevallen gaat het om een menselijke fout: data zijn naar de verkeerde of meerdere personen gestuurd.
! Er lijkt een relatie te liggen tussen zich bewust zijn van het belang van zorgvuldig omgaan met persoonsgegevens en het melden van datalekken: door de cursussen die ook in 2024 zijn gegeven aan medewerkers, en door de intensieve universiteitsbrede campagnes over privacy en security (zie paragraaf 1) is men alerter op eventuele onregelmatige verwerkingen en worden deze makkelijker gemeld. Dit is een positieve ontwikkeling.

Een andere categorie datalekken wordt veroorzaakt doordat medewerkers toegang hebben tot meer (bijzondere) persoonsgegevens dan voor hun functie noodzakelijk is.
Bij het cluster HR en Health, onderdeel van University Services, kwamen de meeste datalekken voor (32 van de 69 totaal).
Een aanzienlijk aantal daarvan had te maken met niet goed ingerichte autorisaties in AFAS, het HRM softwaresysteem waarin alle gegevens van medewerkers en de financiële administratie worden verwerkt. Dit kan ernstige gevolgen hebben voor de integriteit, veiligheid en vertrouwelijkheid.
! Sinds AFAS in 2020 werd ingevoerd, wordt er al gewerkt aan een fijnmaziger autorisatiematrix. Dit is tot op heden nog niet voldoende geëffectueerd.
Hiermee loopt de universiteit een ernstig (privacy) beveiligingsrisico.

Naast dat de persoonsgegevens onrechtmatig verwerkt worden, vindt periodieke evaluatie van toegangsrechten niet of weinig plaats. Hierdoor kunnen inconsistenties of onregelmatigheden in de toegangsrechten mogelijk voortbestaan, wat mogelijkheden biedt voor ongeoorloofde toegang en potentiële beveiligingsinbreuken.
Dit wordt onderschreven door de SURF-audit informatiebeveiliging 2024 door EY; in dit rapport wordt aanbevolen ‘om de implementatie van de autorisatiematrix te versnellen en deze verplicht te stellen binnen het beleid. Dit kan worden gerealiseerd door duidelijke richtlijnen op te stellen, verantwoordelijkheden toe te wijzen en regelmatig audits uit te voeren om de naleving te waarborgen’.

Aanbeveling
Geef prioriteit aan de juiste inrichting van autorisaties door het instellen van een autorisatiematrix, waarin de rollen en bijbehorende taken duidelijk zijn beschreven en ingeregeld. De in 2023 ingestelde werkgroep voor autorisaties heeft nog niet het gewenste resultaat opgeleverd. Het opvolgen en monitoren van de inrichting moet worden belegd volgens het Eigenaarschapsmodel.
Wat betreft datalekken in het algemeen: waarborg dat maatregelen worden opgevolgd door de risico-eigenaar.

9. Samenwerking andere partijen

De universiteit werkt samen met verschillende organisaties waarbij persoonsgegevens worden uitgewisseld en waarbij zowel de universiteit als de andere partij verwerkingsverantwoordelijke kan zijn.
Voorbeelden hiervan zijn het UMCG en de Hanzehogeschool Groningen en diverse consortia bij zowel onderwijs als onderzoek:

- Studenten studeren bij de universiteit en volgen in dat kader coschappen bij het UMCG, waar ze geregistreerd worden
- Studenten studeren bij zowel de universiteit als de Hanze Hogeschool Groningen
- Medewerkers doen een onderzoek binnen een consortium, waarbij data worden gedeeld.

In al deze gevallen worden ook veel persoonsgegevens uitgewisseld.
Vragen hierbij zijn onder andere of duidelijk is waar de verantwoordelijkheden zijn belegd, wie de eigenaar is van de data, of er een doelbinding is en of de juiste afspraken zijn gemaakt over de verwerkingen.

Aanbeveling
Neem de overeenkomsten die ten grondslag liggen aan de samenwerking periodiek onder de loep en actualiseer deze.
Stel het eigenaarschap en de te onderscheiden verantwoordelijkheden van de gezamenlijke verwerkingen vast (in overeenstemming met wat in paragraaf 3 werd beschreven).

10. Nieuwe ontwikkelingen en uitdagingen

Maatschappelijke ontwikkelingen dwingen tot blijvende aandacht voor risicobeheersing van Privacy en Security. Er wordt een tweetal nader belicht.

Artificial Intelligence

Op 1 augustus 2024 is de Artificial Intelligence-Act (AIA) van toepassing geworden. Deze Europese verordening geldt ook in Nederland en beoogt de ontwikkeling en het gebruik van Artificial Intelligence systemen (AI-systemen) te faciliteren, onder voorwaarde dat deze systemen veilig zijn en bij ontwikkeling en gebruik rekening wordt gehouden met (grond)rechten en vrijheden van burgers.
In de AIA wordt bepaald dat met ingang van februari 2025 elke instelling aan ‘’AI- geletterdheid” moet werken. Dit betekent dat medewerkers en studenten van de universiteit de kennis en vaardigheden moeten worden bijgebracht die nodig zijn om goed geïnformeerd gebruik te maken van AI-systemen, bewust te zijn van de risico’s én kansen die gepaard gaan met AI en om schadelijke gevolgen van gebruik van AI-systemen te voorkomen.

Vooruitlopend op deze bepaling is in het najaar van 2024 door het P&S-Gilde de campagne ‘’Veilig werken met AI” gelanceerd. Deze universiteitsbrede awareness campagne geeft medewerkers en studenten een aantal basisinstructies bij het gebruik van AI.
Ook moet de universiteit met ingang van februari 2025 stoppen met het gebruik van verboden AI. Dit verbod betekent feitelijk een verbod op AI-praktijken die grote (maatschappelijke) schade kunnen aanrichten.
Tegelijkertijd worden er binnen de universiteit diverse AI-toepassingen reeds in gebruik genomen en zijn er diverse initiatieven gestart voor ontwikkeling en inkoop van AI-systemen. Dit speelt bij alle domeinen binnen de universiteit,
Om aan de AIA te kunnen voldoen zal de universiteit dus de nodige inspanningen moeten verrichten. Daartoe moet de universiteit zicht hebben op welke AI-systemen er in gebruik zijn en een proces organiseren om aanvragen van AI-systemen te beoordelen.
Om de AI-geletterdheid te bevorderen is een aantal informatiepagina’s en trainingen beschikbaar gemaakt om medewerkers en studenten wegwijs te maken in de risico’s en kansen van het gebruik van AI en er wordt gewerkt aan een integraal AI-programma voor de universiteit. De governance van AI moet nog worden belegd.

Aanbeveling
Leg bij gebruik van AI-toepassingen, in het verlengde van het Eigenaarschapsmodel zoals genoemd in paragraaf 3, vast wie verantwoordelijk is voor de governance en voor de compliance check: toets of bestaande (en toekomstige) toepassingen van AI aan de AIA voldoen en monitor deze. Hierbij kan de P&S-organisatie een ondersteunende rol spelen; P&S-coördinatoren staan dicht bij de mogelijke gebruikers van AI-systemen.
Zij kunnen de nodige actie ondernemen om gebruikers conform de richtlijnen van de universiteit en in overeenstemming met de AIA te laten opereren. Zet in op het gebruik van veilige algoritmes en alternatieven.
Hierbij is het belangrijk te benadrukken dat bij het gebruik van AI niet altijd persoonsgegevens worden verwerkt. Juridische kennis van de AIA en technische kennis van AI-systemen dienen voorhanden te zijn.

Mondiale (beveiligings) bedreigingen met betrekking tot data uitwisseling

Mede door veranderende geopolitieke verhoudingen staat de veilige verwerking van data onder druk. De risico’s nemen toe.
SURF heeft in 2024 een geüpdatet dreigingsbeeld voor de onderwijssector uitgebracht. Dit rapport bevestigt dat er onverminderd sprake is van een hoge dreiging voor de onderwijssector. Bij Kennisveiligheid gaat het om het risico van ongewenste overdracht van sensitieve kennis en technologie naar derdelanden. Dit kan ook gevolgen hebben voor de (sociale) veiligheid van personen en informatiebeveiliging.
Het ministerie OCW heeft in een brief van 27 februari 2024 instellingen opgedragen te werken aan het versterken van hun weerbaarheid tegen statelijke dreigingen door kennisveiligheidsbeleid te implementeren.

Aanbeveling
Stel richtlijnen op voor het delen van persoonsgegevens met partijen in landen buiten de Europese Unie en waarborg dit proces adequaat. Gebruik het verwerkingsregister (zoals genoemd in paragraaf 5) om de verwerkingen naar zogenaamde derdelanden in kaart te brengen en monitor deze, in overeenstemming met sectorale richtlijnen, zoals die van SURF. Maak gebruik van de informatie van het landelijke Loket Kennisveiligheid, dat door de overheid is ingesteld.

Tot slot

Maatschappelijke ontwikkelingen dwingen tot blijvende aandacht voor risicobeheersing ten aanzien van Privacy en Security. Het betreft nagenoeg alle processen en systemen die binnen de universiteit worden uitgevoerd. De naleving en uitvoering van wet- en regelgeving met betrekking tot bescherming van persoonsgegevens is essentieel om aan de verantwoordingsplicht te kunnen voldoen die uit de AVG voortvloeit.

!

Met het opgestelde beleid ten aanzien van de inrichting van de Privacy & Security-organisatie en de investering die hiermee gepaard gaat, laat het CvB duidelijk commitment zien.
Het College heeft uitgesproken dat ondanks dat de universiteit wordt bedreigd met kortingen op de begroting, bezuinigingen op personeelsformatie voor Privacy & Security-zaken niet zijn toegestaan.

Een bijzondere omstandigheid is dat ik, de schrijver van dit verslag, tot mijn vertrek in 2020, als juridisch beleidsmedewerker Privacy en Security verbonden was aan de universiteit en daar meewerkte aan de implementatie van de AVG in 2018.
In oktober 2024 ben ik als interim-FG aangesteld. Ik kijk hierdoor als een relatieve buitenstaander naar de ontwikkeling die de universiteit in vier jaar tijd heeft doorgemaakt om de Privacy & Security-organisatie vorm te geven.

!

En die ontwikkeling is fors; wat ik met name signaleer is dat er een breder universitair draagvlak is gecreëerd. Was er in 2020 zowel bij medewerkers als het hoger management vooral weerstand en onverschilligheid ten aanzien van de implementatie van de AVG (”we mogen helemaal niets meer, wat geeft dit weer veel extra werk, waar is dat allemaal voor nodig?”), nu zie ik een robuuste P&S-organisatie, met een kern van professionals die zich enorm inzet om het veilig omgaan met persoonsgegevens vanzelfsprekend te maken èn op een hoger plan te brengen.
Ook is er een grote betrokkenheid en commitment van het hoger management, met name het CvB. Door de keuze van het CvB om financieel en organisatorisch te investeren in een tweejarig Programma om Privacy & Security in de hele organisatie te verankeren, is het volwassenheidsniveau van 2.1 in 2020 tot 2.5 in 2023 met sprongen vooruitgegaan. Een stap van 2.5 naar 2.8 zal in verhouding moeilijker te realiseren zijn dan die van 2.1 naar 2.5.
Dit komt doordat de zaken die nu gerealiseerd moeten worden complexer zijn en dus meer tijd en inspanning vragen van de organisatie, zoals in dit verslag is aangegeven.
Het laaghangend fruit is al geplukt…

Door alle initiatieven binnen alle geledingen van de universiteit, van trainingen tot de herinrichting van processen, van awareness activiteiten tot het maken van werkplannen en beleid, wordt elke medewerker en student binnen de universiteit geïnformeerd over- en aangesproken op het veilig omgaan met persoonsgegevens.
Privacy & Security is een onlosmakelijk onderdeel geworden van ieders werk en studie.
Dat is een enorme winst!

Prioritering

Zoals aangegeven in dit verslag is de materie complex. Onder andere door de onderlinge afhankelijkheden zullen de laatste stappen die genomen moeten worden veel inspanning vergen. De hoogste risico's die in kaart zijn gebracht hebben allemaal betrekking op compliance hiaten.

Aanbeveling
onderneem de volgende gerichte actie op de hoogste risico's, met als doel aan het eind van het jaar 2025 de genoemde stappen met positief resultaat- risico's zijn gemitigeerd- te kunnen afronden:

- Het Eigenaarschapsmodel uitrollen, te beginnen bij de twee grote administratieve systemen voor medewerkers en studenten, en de processen die daarbij ondersteund worden
- Autorisaties op juiste wijze inrichten binnen het administratieve systeem voor medewerkers
- Bewaartermijnen bepalen en de verantwoordelijken voor de belangrijkste Top-20 van administratieve systemen opdragen de bezwaartermijnen in te richten in samenwerking met het Volwassenheidsprogramma Informatiebeheer
- Opdracht geven om een universiteitsbreed RDMP-tool te realiseren waarin informatie over de verwerking van persoonsgegevens in onderzoek wordt vastgelegd

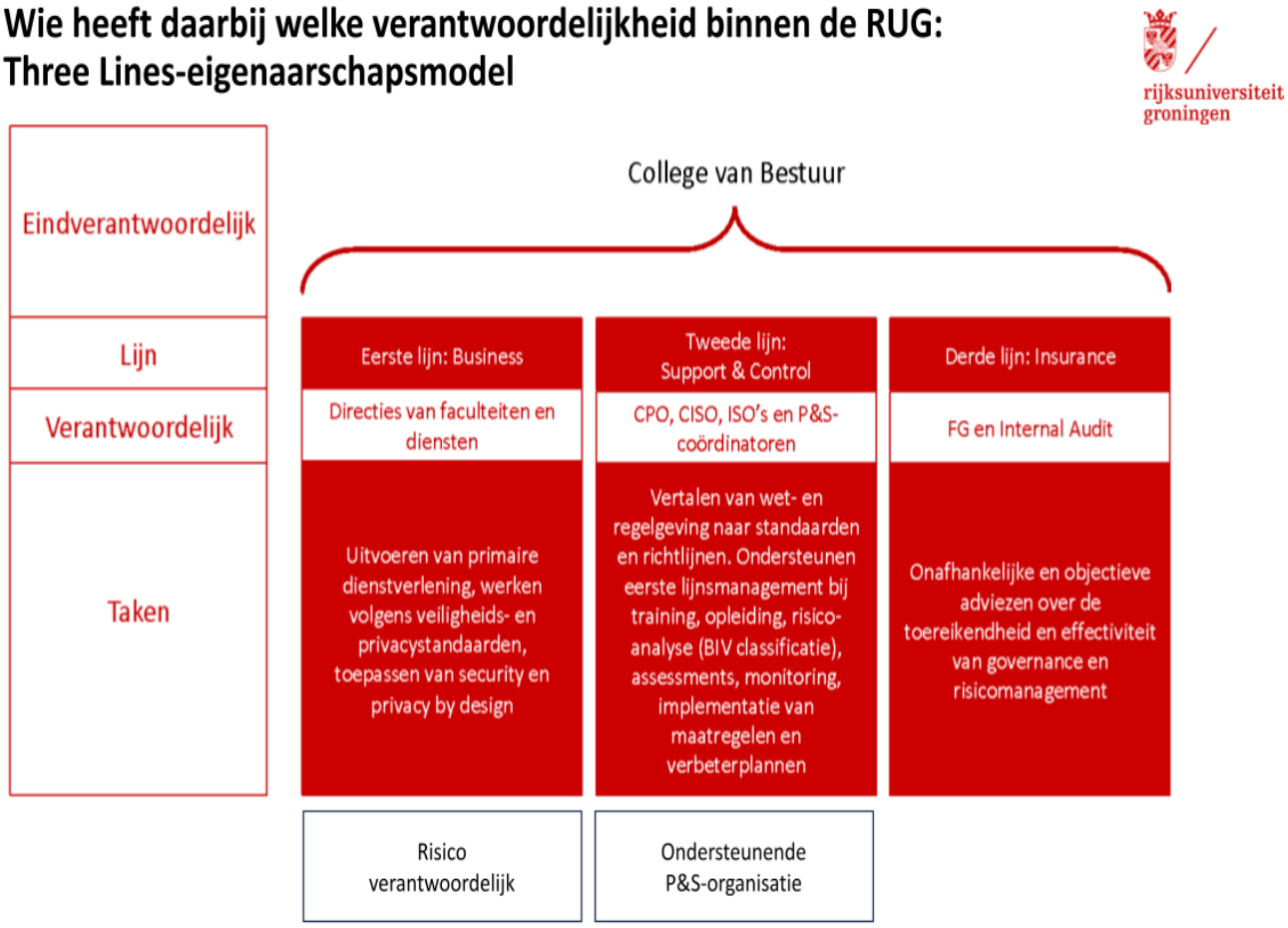
Leg vast wie eindverantwoordelijk is en welk resultaat binnen welke termijn moet worden bereikt. De verantwoordelijke rapporteert per kwartaal over de voortgang aan het College.

En, de zwakste schakel bepaalt uiteindelijk of en wanneer het gewenste volwassenheidsniveau gehaald wordt. Dat betekent ook dat als er geïnvesteerd wordt in een aantal zaken die nu in verhouding achterblijven, er nog enorme voorwaartse stappen te maken zijn.

De FG zal vanuit diens rol blijven toezien op mogelijkheden tot aanscherping en verbeteringen van maatregelen om het geambieerde volwassenheidsniveau van 3.0 mogelijk te maken.

Bijlagen

Bijlage 1:
Drie-lijns Eigenaarschapsmodel



Bijlage 2:

Voorbeeld weergave volwassenheidsniveau in Eramba ‘’spinnenweb”:

