

ALGEMEEN BELEID BESCHERMING PERSOONSGEGEVENS

RIJKSUNIVERSITEIT GRONINGEN

Versie 4 – 26 mei 2026 - vastgesteld door het College van Bestuur

Auteur: mr. J.W. Oordt - Chief Privacy Officer

Inhoud

1. Definities gebruikte begrippen.....	4
2. Uitgangspunten.....	5
2.1. Inleiding	5
2.2. Privacy-visie Rijksuniversiteit Groningen	5
2.3. Doel	5
2.4. Doelgroep	6
2.5. Toepassingsbereik.....	6
2.6. Raakvlakken met en verhouding tot andere beleidsthema's en beleidsstukken	6
2.7. Juridisch kader.....	7
2.8. Ingangsdatum en onderhoud.....	7
3. Governance van privacy	8
3.1. Three lines model, samenhang Privacy & Security (P&S)	8
3.2. Verantwoordelijkheden en bevoegdheden faculteitsbestuur / directies diensten.....	9
3.3. Verantwoordelijkheden en bevoegdheden College van Bestuur.....	10
3.4. Verantwoordelijkheden en bevoegdheden privacy & security-coördinatoren, P&S-Gilde en medewerkers	10
3.4.1. Algemeen.....	10
3.4.2. Verantwoordelijkheden en bevoegdheden privacy & security-coördinatoren..	11
3.4.3. Verantwoordelijkheden en bevoegdheden P&S Gilde	11
3.4.4. Verantwoordelijkheden en bevoegdheden medewerkers	11
3.4.5. Verantwoordelijkheden en bevoegdheden van onderzoekers	11
3.4.6. Verantwoordelijkheden en bevoegdheden van studenten	11
3.5. Verantwoordelijkheden en bevoegdheden CPO, AJZ en CISO	12
3.5.1. Verantwoordelijkheden en bevoegdheden CPO.....	12
3.5.2. Verantwoordelijkheden en bevoegdheden AJZ	12
3.5.3. Verantwoordelijkheden en bevoegdheden CISO	13
3.6. Verantwoordelijkheden en bevoegdheden FG en IT-auditor	13
3.6.1. Verantwoordelijkheden en bevoegdheden FG	13
3.6.2. Verantwoordelijkheden en bevoegdheden IT-auditor	14
3.7. Verantwoordelijkheden en bevoegdheden Commissie Privacy, Security en Informatiebeheer.....	14
3.8. Verantwoordelijkheden en bevoegdheden medezeggenschapsorganen.....	14

4. Toepassing privacybeleid	14
4.1. Werkprogramma privacyvolwassenheid College van Bestuur, beleidsevaluatie, nader privacybeleid, protocollen	14
4.2. PDCA-cyclus gegevensbeschermingfaculteiten en diensten.....	15
4.3. Privacy by Design & by default, DPIA's.....	15
4.4. Gedragscodes en certificeringen	16
4.5. Register voor de verwerkingsactiviteiten	16
4.6. Informatiebeveiliging	16
4.7. Privacy-incidenten, datalekken.....	16
4.8. Verwerking van persoonsgegevens van de RUG door of samen met derden	17
4.9. Doorgifte van persoonsgegevens naar buiten de EER	17
4.10. Transparantie en rekenschap.....	17
4.10.1. Privacyverklaring	17
4.10.2. Rechten van de betrokkene	17
4.10.3. Verantwoording aan privacytoezichthouders	18
4.11. Communicatie en PR.....	18
4.12. Bewustwording en training	18
4.13. Aard van dit privacybeleid	18
5. Protocollen en nader privacybeleid.....	18

1. Definities gebruikte begrippen

De in dit privacybeleid gehanteerde begrippen worden als volgt gedefinieerd:

- AJZ: de afdeling Algemene en Juridische Zaken van de RUG;
- AVG: de Algemene verordening gegevensbescherming;
- Betrokkene: de natuurlijke persoon van wie persoonsgegevens worden verwerkt;
- CISO: de Chief Information Security Officer van de RUG;
- CPO: de Chief Privacy Officer van de RUG;
- Commissie Privacy, Security & Informatiebeheer: de strategische commissie die het CvB adviseert over de toepassing van dit privacybeleid in relatie tot de strategische doelen van de RUG;
- CvB: het College van Bestuur van de RUG;
- Digital Competence Centre (DCC): een samenwerking van de Universiteitsbibliotheek en het Centrum voor Informatietechnologie van de RUG ter ondersteuning onderzoekers en onderzoeksinstituten bij datamanagement;
- DPIA: Data Protection Impact Assessment (Nederlands: Gegevensbeschermingseffectbeoordeling), een beoordeling van de privacy-impact van een proces of systeem waarbinnen persoonsgegevens worden verwerkt;
- FG: de Functionaris voor gegevensbescherming van de RUG;
- GRC-tool: de digitale omgeving voor Governance, Risk & Compliance, waarin P&S-risico's en mitigerende maatregelen worden geregistreerd en gemonitord;
- P&S-Gilde: het samenwerkingsverband en overlegorgaan van P&S-coördinatoren;
- Persoonsgegevens: alle gegevens die betrekking hebben op een natuurlijk persoon en deze persoon direct of indirect identificeren;
- Privacyvolwassenheid: het voldoen aan de Privacywet- en regelgeving en het waarborgen van een zorgvuldige en behoorlijke omgang met persoonsgegevens;
- Privacy & security-coördinator: de medewerker van de RUG die door een faculteitsbestuur of directie van een dienst is aangewezen om de privacyvolwassenheid van een faculteit, dienst of een afdeling daarvan te coördineren;
- Privacyverklaring: de verklaring, formulier voor informed consent of een ander document waarin de betrokkene wordt geïnformeerd over de verwerking van diens persoonsgegevens door de RUG;
- Privacywet- en regelgeving: alle nationale of internationale wet- en regelgeving die van toepassing is op de RUG en voorwaarden stelt ten aanzien van het verwerken van persoonsgegevens, waaronder de AVG;
- Privacybeleid: onderhavig algemeen beleid bescherming persoonsgegevens;;
- Privacy-impact: de nadelige gevolgen van een proces of verwerking voor de zorgvuldige en behoorlijke omgang met persoonsgegevens en voor de bescherming van de persoonlijke levenssfeer van een betrokkene;
- RUG: Rijksuniversiteit Groningen;
- Verwerking, verwerken: iedere handeling/ieder handelen met betrekking tot persoonsgegevens, zoals inzien, delen, wijzigen, kopiëren, opslaan en vernietigen;
- Verwerker: iedere (rechts)persoon of organisatie die namens de RUG persoonsgegevens verwerkt.

2. Uitgangspunten

2.1. Inleiding

Door toenemende digitalisering en door toenemende bewustwording van het belang van de bescherming van de persoonlijke levenssfeer van een individu, is privacy een steeds relevanter onderwerp geworden. Een onderdeel van het recht op bescherming van de persoonlijke levenssfeer is het recht op bescherming van persoonsgegevens. Hieruit vloeit voor de Rijksuniversiteit Groningen (RUG) de verplichting voort tot zorgvuldige omgang met persoonsgegevens van studenten, onderzoekssubjecten, medewerkers en ieder ander van wie zij persoonsgegevens verwerkt. Het College van Bestuur van de RUG (hierna: CvB) wil dat deze verplichting tot in de haarvaten van de universiteit wordt toegepast. Daartoe heeft het CvB onderhavig beleid (hierna: Privacybeleid) vastgesteld dat in hoofdlijnen de visie, uitgangspunten en governance ten aanzien van de bescherming van persoonsgegevens beschrijft.

2.2. Privacy-visie Rijksuniversiteit Groningen

De RUG heeft als missie het genereren, delen en behouden van kennis en informatie, met als doel bij te dragen aan het oplossen van maatschappelijke en wetenschappelijke uitdagingen. De RUG wil zo een impactvolle bijdrage aan de samenleving leveren. De RUG hanteert een privacy-visie die hierop aansluit. Deze visie luidt als volgt.

Elke student, elke medewerker, elk onderzoekssubject en ieder ander die op enigerlei wijze is verbonden met de RUG moet erop kunnen vertrouwen dat zijn of haar persoonsgegevens door de RUG rechtmatig worden verwerkt en passend worden beschermd. Te allen tijde gaat de RUG zorgvuldig en behoorlijk om met de persoonsgegevens die zij verwerkt. Door te voldoen aan de geldende privacywet- en regelgeving biedt de RUG een consistent en hoog niveau van bescherming van de rechten en vrijheden van individuen ('privacyvolwassenheid').

De RUG is daarom transparant over wat zij met persoonsgegevens doet en neemt verantwoordelijkheid, ook als er fouten worden gemaakt. De RUG stelt individuen in staat hun gegevens in te zien en te corrigeren. Hun vragen en eventuele klachten worden serieus genomen en op een correcte manier afgehandeld.

Binnen dit kader wordt excelleren in onderwijs en onderzoek zo veel mogelijk gefaciliteerd en gerealiseerd. Privacyvolwassenheid betaalt zich uit in een positieve bijdrage aan de missie van de RUG.

2.3. Doel

Doel van dit privacybeleid is:

- Het waarborgen van een zorgvuldige, behoorlijke en veilige omgang met de persoonsgegevens die de RUG verwerkt, in overeenstemming met de geldende privacywet- en regelgeving, op een zodanige manier dat de rechten en vrijheden van individuen worden geëerbiedigd;

- Het scheppen van de kaders waarbinnen dit beleid uitgevoerd wordt;
- Het voorkomen van privacy-incidenten en, als deze zich toch voordoen, het beperken van schade voor individuen en de organisatie;
- Het implementeren van maatregelen en mechanismen die de privacyvolwassenheid van de RUG optimaliseren;
- Het faciliteren en activeren van alle medewerkers van de RUG om bij te dragen aan de privacyvolwassenheid van de organisatie;
- Het in staat stellen van het CvB om met vertrouwen verantwoording af te leggen aan betrokkenen en autoriteiten.

2.4. Doelgroep

De doelgroep van de verplichtingen in dit beleid wordt gevormd door alle medewerkers en studenten van de RUG. De verantwoordelijkheden, taken en bevoegdheden die medewerkers en studenten hebben met betrekking tot de bescherming van persoonsgegevens, zijn nader uitgewerkt in dit privacybeleid. Het beleid wordt ten behoeve van de transparantie over verwerking van persoonsgegevens gedeeld op de publieke website van de RUG.

2.5. Toepassingsbereik

Dit privacybeleid is van toepassing op de verwerking van persoonsgegevens. Persoonsgegevens zijn alle gegevens die betrekking hebben op een natuurlijk persoon en die deze persoon direct of indirect identificeren. Een verwerking betreft iedere handeling met betrekking tot persoonsgegevens, zoals inzien, delen, wijzigen, kopiëren, opslaan en vernietigen. Het beleid heeft betrekking op de gehele levenscyclus van persoonsgegevens, dus vanaf het moment van verzameling of creatie van persoonsgegevens tot de verwijdering of vernietiging ervan. Het beleid geldt ten aanzien van zowel geautomatiseerde als niet-geautomatiseerde verwerkingen.

Het beleid is van toepassing op de gehele universiteit. Het is gericht op alle processen van de universiteit waarbij persoonsgegevens worden verwerkt, zowel in het kader van onderwijs en onderzoek als in het kader van de bedrijfsvoering die deze primaire taken faciliteert en ondersteunt. Wanneer de verwerking van persoonsgegevens wordt verricht door een derde in opdracht van de RUG, gezamenlijk met de RUG of anderszins door of vanwege de universiteit, is dit beleid eveneens van toepassing.

2.6. Raakvlakken met en verhouding tot andere beleidsthema's en beleidsstukken

Dit privacybeleid heeft raakvlakken met andere beleidsterreinen binnen de RUG, zoals informatiebeveiliging, *Artificial Intelligence* en archivering. Dit privacybeleid is zoveel mogelijk in lijn gebracht met het voor die terreinen opgestelde beleid. Het is echter mogelijk dat in ander beleid andere accenten worden gelegd ten aanzien van de bescherming van persoonsgegevens. Deze moeten altijd in het licht van dit privacybeleid beoordeeld worden.

2.7. Juridisch kader

Het juridisch kader voor dit privacybeleid wordt hoofdzakelijk gevormd door de Algemene Verordening Gegevensbescherming (AVG). Daarnaast bestaat nationale uitvoeringswetgeving (bijv. de Nederlandse Uitvoeringswet AVG) en wetgeving die regels stelt voor specifieke vormen van verwerkingen van persoonsgegevens. Verder is op de RUG wetgeving van toepassing die specifieke instructies ten aanzien van een verwerking kan geven, zoals bewaarplichten of anonimiseringsplichten (denk aan de Archiefwet en de Wet Open Overheid). Daarnaast is in voorkomende gevallen overige wetgeving waaraan de RUG zich dient te houden (bijv. de Wet op het Hoger onderwijs en onderzoek, de Algemene wet bestuursrecht en de AI-Verordening) onderdeel van het juridisch kader. Het voert echter te ver om de verhouding tussen de verschillende wetgeving nader te bepalen in dit beleid. Dit zal bij toepassing van geval tot geval beoordeeld worden.

Naast de toepasselijke wetgeving wordt het juridisch kader bepaald door beleidsregels, gedragscodes en certificeringsmechanismen die door een bevoegde overheidsinstantie (bijvoorbeeld de Autoriteit Persoonsgegevens of de Europese Commissie) zijn vastgesteld. Dit geldt eveneens voor zienswijzen van de Functionaris voor de Gegevensbescherming (hierna: FG). Ook kunnen gedragscodes worden opgesteld vanuit koepels als de UNL (bijv. gedragscode voor gebruik van persoonsgegevens in wetenschappelijk onderzoek) of door de RUG zelf, waaraan de universiteit zich committeert.

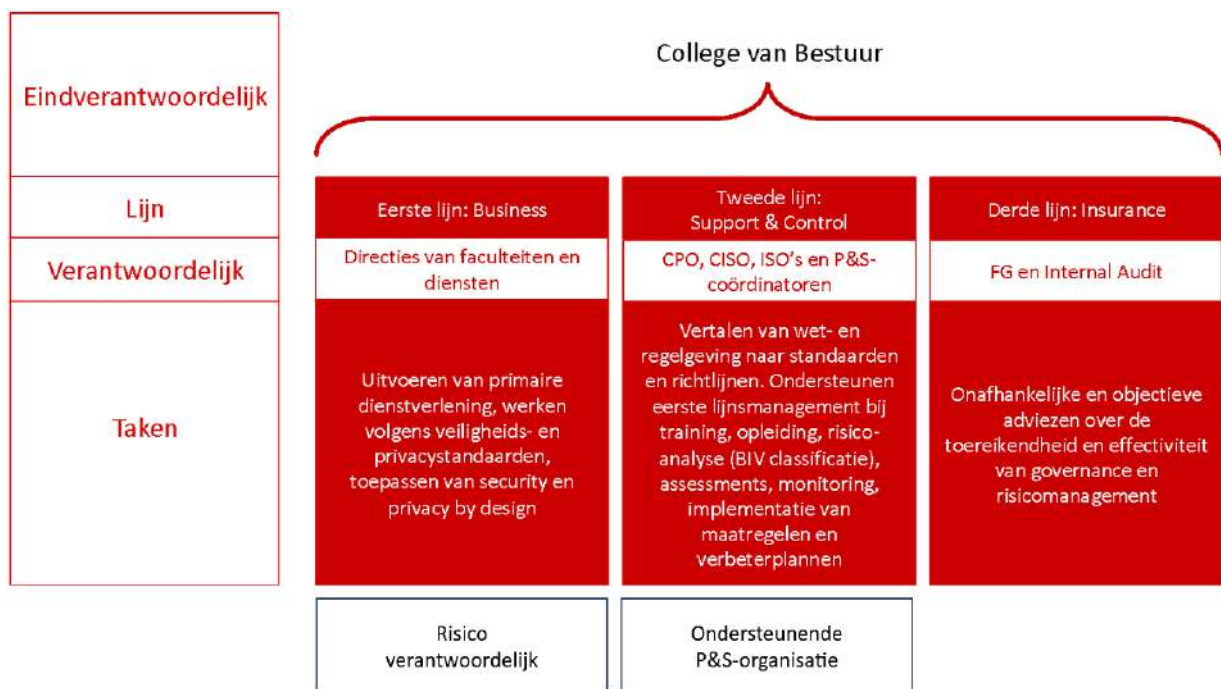
2.8. Ingangsdatum en onderhoud

De eerste versie van dit privacybeleid is vastgesteld op 4 juni 2018 door het CvB en is vanaf dat moment van toepassing. Het beleid zal minimaal eens per twee jaar worden geactualiseerd en aangevuld. Wijzigingen zijn van kracht na goedkeuring door het CvB.

3. Governance van privacy

3.1. Three lines model, samenhang Privacy & Security (P&S)

De governance van privacy is in samenhang met informatiebeveiliging georganiseerd. *Privacy & Security* (P&S) zijn zodoende bij de RUG zeer nauw met elkaar verweven, niet alleen inhoudelijk maar ook organisatorisch. De governance is opgetuigd volgens het zogenaamde “three lines model”¹. Door middel van dit model zijn de verschillende rollen, verantwoordelijkheden en relaties beschreven ten aanzien van het opstellen van beleid en maatregelen, het nemen van maatregelen en toetsing en controle van deze maatregelen voor P&S. Het model is schematisch weergegeven in figuur 1.



Figuur 1. Governancestructuur Privacy & Security

1^e lijn

Het ‘three lines’ model hanteert als uitgangspunt dat de faculteitsbesturen en directies van diensten (‘de *business*’) verantwoordelijk zijn voor de inrichting van de eigen processen. Privacy en informatiebeveiliging maken hier integraal onderdeel van uit. De besturen en directies worden hierbij ondersteund door P&S-coördinatoren.

2^e lijn

De CISO en CPO brengen aan het College van Bestuur voorstellen uit voor beleid en maatregelen op het gebied van informatiebeveiliging en privacy. Zij ondersteunen en adviseren de 1^e lijn en toetsen of deze diens verantwoordelijkheid ten aanzien van informatieveiligheid en gegevensbescherming neemt.

¹ Three lines model of The Institute of Internal Auditors (IIA), [Three Lines Model Updated - ENG \(iaa.nl\)](https://www.iaa.nl/en/three-lines-model).

3^e lijn

De 3^e lijn is een onafhankelijke controle op het samenspel tussen de eerste en tweede lijn en geeft daarover een objectief, onafhankelijk oordeel met mogelijkheden tot verbetering. De controle kan worden uitgevoerd door de FG, een interne IT-auditor en/of door een externe auditor.

Een nadere uitwerking van deze verantwoordelijkheden in omvang, taken en bevoegdheden wordt in het vervolg van dit beleid gegeven. Te allen tijde zal het bestuur of de directie, waaronder een P&S-functionaris ressorteert, deze persoon tijdig betrekken en de middelen en tijd geven om de functie naar behoren uit te voeren.

3.2. Verantwoordelijkheden en bevoegdheden faculteitsbestuur / directies diensten

De faculteitsbesturen en de directies van de diensten van de RUG zijn ervoor verantwoordelijk dat hun faculteit of dienst voldoet aan de privacywetgeving en dit privacybeleid. Het bestuur of de directie draagt de volgende de taken en verantwoordelijkheden:

- Zorgdragen voor bewustwording van het belang van privacyvolwassenheid en de bescherming van persoonsgegevens binnen de faculteit of dienst;
- Het in kaart brengen van alle verwerkingen van persoonsgegevens binnen diens faculteit of dienst, het registreren van deze verwerkingen in het daarvoor bestemde register en het actueel houden van deze registraties;
- Het in kaart brengen van de risico's voor de bescherming van persoonsgegevens die spelen bij de verwerkingen van de organisatie-eenheid en het beoordelen en mitigeren van deze risico's;
- Zorgdragen dat de verwerkingen van persoonsgegevens van de faculteit of dienst in overeenstemming zijn met de privacywet- en regelgeving;
- Zorgdragen dat een DPIA wordt uitgevoerd wanneer dat nodig is op grond van de privacywet- en regelgeving en/of RUG-beleid;
- Het, op basis van een DPIA of andere risicoanalyse, realiseren van passende waarborgen voor de bescherming van persoonsgegevens en het implementeren van passende technische en organisatorische maatregelen;
- Het monitoren en verbeteren van de privacyvolwassenheid van diens faculteit of dienst;
- Het tijdig en volledig melden van (vermoedelijke) datalekken en privacy-incidenten binnen de faculteit of dienst;
- Het, binnen het P&S-Gilde, afstemmen met andere faculteiten en diensten over de toepassing van dit beleid, zodat dubbel werk voorkomen wordt;
- Het minimaal jaarlijks informeren van de faculteitsraad of dienstraad over de stand van zaken met betrekking tot bovenstaande activiteiten.

Het bestuur of de directie werkt bovenstaande verantwoordelijkheden voor de domeinen onderwijs, bedrijfsvoering en wetenschappelijk onderzoek uit in concrete maatregelen en acties. Risico's voor gegevensbescherming, maatregelen en acties worden, volgens het P&S-

risicomanagementbeleid en het protocol risico's en maatregelen P&S, geregistreerd in de *GRC-tool* van de RUG. Hiermee wordt grip en zicht op risico's, borging van een verbetercyclus en de samenwerking tussen faculteiten en diensten wordt gefaciliteerd.

Privacy is een zelfstandig aandachtsgebied van een faculteitsbestuur of directie. Indien een faculteitsbestuur of een directie uit meerdere personen bestaat, wordt vastgesteld welk bestuurslid privacy in portefeuille heeft. Het bestuur of de directie zorgt voor voldoende bemensing ten behoeve van de uitvoering van bovenstaande verantwoordelijkheden en taken en stelt minimaal één privacy & security-coördinator aan om de toepassing van de privacywet- en regelgeving en dit privacybeleid binnen diens faculteit of dienst te coördineren.

De faculteitsbesturen en directies van diensten leggen over de uitvoering van bovenstaande verantwoordelijkheden verantwoording af aan het CvB. Jaarlijks beoordelen de CPO, CISO namens het CvB, of de faculteit of dienst voldoet aan de eisen van dit privacybeleid en het P&S-risicomanagementbeleid.

3.3. Verantwoordelijkheden en bevoegdheden College van Bestuur

Het CvB is eindverantwoordelijk voor het beheer van de universitaire gegevensbestanden en de privacyvolwassenheid van de Rijksuniversiteit Groningen. Het CvB vertegenwoordigt de RUG richting externe toezichthouders, de betrokkene en derden. Verder informeert het CvB de universiteitsraad en de Raad van Toezicht waar nodig over de ontwikkelingen op dit vlak. Het CvB kan zich bij het afleggen van verantwoording en het geven van informatie laten ondersteunen door de FG, CPO en CISO. Het CvB draagt er zorg voor dat de FG tijdig en in voldoende mate wordt betrokken bij aangelegenheden die de bescherming van persoonsgegevens betreffen.

Het CvB stelt iedere twee jaar, op basis van een voorstel van de CPO, vast hoe de RUG verder dient te groeien op het gebied van privacyvolwassenheid. Het CvB neemt daarbij de aanbevelingen die de FG uitbrengt in acht. Afwijken van deze aanbevelingen gebeurt met deugdelijke motivering. Het CvB faciliteert de gremia en medewerkers van de RUG in het voldoen aan de privacywet- en regelgeving en stelt hiervoor middelen en ondersteuning beschikbaar. Wanneer een faculteitsbestuur of directie van een dienst in gebreke is met betrekking tot de privacywet- en regelgeving of dit privacybeleid, treft het CvB in redelijkheid de maatregelen of sancties om dit te herstellen.

3.4. Verantwoordelijkheden en bevoegdheden privacy & security-coördinatoren, P&S-Gilde en medewerkers

3.4.1. Algemeen

Privacy & security-coördinatoren, onderzoekers en overige medewerkers werken onder verantwoordelijkheid van het faculteitsbestuur of directie van de dienst waar zij onder ressorteren.

3.4.2. Verantwoordelijkheden en bevoegdheden privacy & security-coördinatoren

De privacy & security-coördinator is het eerste aanspreekpunt voor privacygerelateerde vragen van de medewerkers van de faculteit of dienst. Tevens brengt de coördinator de verwerkingen van persoonsgegevens in kaart en registreert hij of zij deze in het daarvoor bestemde register. De privacy- & securitycoördinator ondersteunt de collega's van de faculteit of dienst bij het uitvoeren van DPIA's en het opstellen en beoordelen van privacy-overeenkomsten. De privacy & security-coördinator legt verantwoording af aan diens bestuur dan wel directie.

3.4.3. Verantwoordelijkheden en bevoegdheden P&S Gilde

Het Privacy & Security Gilde (P&S Gilde) is het samenwerkingsverband en overlegorgaan van de P&S-coördinatoren van de RUG. Het P&S-Gilde bewaakt dat faculteiten en diensten waar mogelijk samenwerken aan de behandeling van P&S-vraagstukken en het mitigeren van P&S- risico's. Het P&S-Gilde prioriteert de aanpak van deze vraagstukken en faculteits- en dienstoverstijgende risico's en zorgt voor universiteitsbreed toepasbare oplossingen. Het P&S-Gilde houdt bij het ontwikkelen en uitvoeren van maatregelen zoveel mogelijk rekening met de praktische, alledaagse realiteit van medewerkers en studenten. Het P&S-Gilde zorgt voor universiteitsbrede awarenesscampagnes ten behoeve van het vergroten van de kennis en vaardigheden van personeel en studenten. De CPO en de CISO zitten de overleggen van het P&S-Gilde voor en begeleiden de uitvoering van bovenstaande taken.

3.4.4. Verantwoordelijkheden en bevoegdheden medewerkers

Alle medewerkers van de RUG hebben de verantwoordelijkheid om zorgvuldig om te gaan met de persoonsgegevens die zij verwerken. Ze nemen kennis van de hiervoor opgestelde beleidsstukken, protocollen en instructies en leven die na. Zij ondersteunen waar nodig en mogelijk de P&S-organisatie met hun kennis en kunde. Wanneer zij kennisnemen van mogelijke privacy-incidenten, rapporteren zij deze zo snel mogelijk bij de daarvoor ingerichte meldpunten of de FG.

3.4.5. Verantwoordelijkheden en bevoegdheden van onderzoekers

De onderzoeker heeft een zelfstandige verantwoordelijkheid voor de privacyvolwassenheid van diens onderzoek. Bij de invulling van deze verantwoordelijkheid is een rol weggelegd voor de ethische commissies. Zij zien, namens het faculteitsbestuur, toe op de toetsing van het onderzoek aan ethische en juridische eisen. De onderzoeker conformeert zich aan de privacywet- en regelgeving, (ethische) richtlijnen en gedragscodes in het veld en facultair beleid. Ondersteuning vindt, naast de reguliere ondersteuning binnen de faculteit, plaats door het Digital Competence Centre (hierna: DCC).

3.4.6. Verantwoordelijkheden en bevoegdheden van studenten

Het kan voorkomen dat studenten van de RUG in het kader van hun opleiding toegang krijgen tot persoonsgegevens. Studenten gaan zorgvuldig met de persoonsgegevens om en conformeren zich aan universitair beleid en de instructies die zij ontvangen van hun docenten

en begeleiders. Faculteiten zijn verantwoordelijk voor het begeleiden van studenten bij het gebruik van persoonsgegevens.

3.5. Verantwoordelijkheden en bevoegdheden CPO, AJZ en CISO

3.5.1. Verantwoordelijkheden en bevoegdheden CPO

De Chief Privacy Officer (CPO) is verantwoordelijk voor het ontwikkelen en implementeren van het universitaire privacybeleid, met inbegrip van richtlijnen en procedures voor het beschermen van persoonsgegevens van studenten, personeel, onderzoekssubjecten en andere individuen. De CPO bewaakt dat de faculteit en diensten handelen volgens dit beleid en dat de daaruit vloeiende maatregelen toegepast worden. De CPO geeft faculteiten en diensten advies bij het in kaart brengen en behandelen van risico's en geeft de privacy- & securitycoördinatoren inhoudelijke ondersteuning. De CPO adviseert het CvB over de opvolging van de jaarrapportage van de FG en de toepassing van diens adviezen. De CPO stuurt, samen met de CISO, het P&S-Gilde aan. De CPO stelt iedere twee jaar, in samenwerking met het P&S-Gilde, een werkprogramma op dat beschrijft hoe de RUG verdere privacyvolwassenheidsgroei bereikt.

De CPO adviseert over complexe privacy-aangelegenheden, initieert risico-analyses en privacy-audits, organiseert awarenessprogramma's, en adviseert bestuur en management. De CPO zorgt voor overzicht van en sturing op de privacyrisico's die spelen binnen de universiteit. De CPO rapporteert over diens werkzaamheden aan de Commissie Privacy, Security & Informatiebeheer en is werkzaam bij de afdeling AJZ.

3.5.2. Verantwoordelijkheden en bevoegdheden AJZ

AJZ adviseert faculteiten en diensten bij de toepassing van de privacywet- en regelgeving binnen de RUG. AJZ ondersteunt faculteitsbesturen, directies van diensten en hun privacy- en securitycoördinatoren bij het opstellen van DPIA's, (privacy)overeenkomsten en privacyverklaringen. AJZ ondersteunt de FG bij de uitvoering van diens taken. AJZ adviseert bij nadere uitwerking van dit privacybeleid. Bij AJZ is een coördinator voor de awareness- en trainingsactiviteiten op P&S-gebied werkzaam. Deze functionaris ondersteunt de P&S-coördinatoren, het P&S-Gilde, de CPO en de CISO bij het plannen en uitvoeren van activiteiten die de kennis en vaardigheden van medewerkers en studenten op P&S-gebied vergroten.

AJZ werkt modelovereenkomsten uit die door medewerkers van de RUG kunnen worden gebruikt voor het maken van afspraken met derden ten behoeve van de zorgvuldige en veilige uitwisseling en verwerking van persoonsgegevens. Het daadwerkelijk afsluiten van de overeenkomsten dient altijd te gebeuren conform de instructies van AJZ. Ondertekening gebeurt door of namens het CvB. AJZ zorgt voor een proces waarmee de naleving van de gemaakte afspraken wordt gemonitord.

AJZ stemt haar werkzaamheden op het gebied van privacy voortdurend af met de FG, CPO en de CISO.

3.5.3. Verantwoordelijkheden en bevoegdheden CISO

De CISO is verantwoordelijk voor het ontwikkelen en implementeren van een informatiebeveiligingsprogramma, dat beleid, maatregelen en procedures omvat die zijn ontworpen om de informatiesystemen van de RUG te beschermen tegen interne en externe bedreigingen. De CISO bewaakt het functioneren van het Information Security Management System (ISMS) en houdt toezicht op de naleving van het informatiebeveiligingsbeleid en de daaruit voortvloeiende maatregelen binnen de hele organisatie, adviseert over complexe beveiligingsvraagstukken, initieert risicoanalyses en beveiligingsaudits, organiseert security awareness programma's en adviseert het College van Bestuur, faculteitsbesturen en directies van diensten.

De CISO adviseert, zo nodig samen met de CPO, de FG en/of de IT-auditor, het bestuur van de RUG over de security risico's van de faculteiten en diensten voor informatiebeveiliging en privacybescherming. De CISO geeft inhoudelijk sturing aan het Security Team en het Security Operations Center (SOC). Daarnaast is de CISO voorzitter van Cybersecurity Incident Response Team (CSIRT) van de RUG.

3.6. Verantwoordelijkheden en bevoegdheden FG en IT-auditor

3.6.1. Verantwoordelijkheden en bevoegdheden FG

De FG is verantwoordelijk voor het geven van gevraagd en ongevraagd advies aan het CvB over en het toezicht houden op de naleving van de privacywet- en regelgeving en het privacybeleid. De FG heeft binnen de RUG minimaal de taken, verantwoordelijkheden en bevoegdheden die de privacywet- en regelgeving de FG toekent.

De FG heeft toegang tot alle informatie van de RUG die betrekking heeft op verwerking van persoonsgegevens – zowel tot de persoonsgegevens zelf als tot de verwerkingsactiviteiten en de systemen waarmee die activiteiten worden verricht. Het CvB kan bepalen dat, voordat toegang tot bepaalde informatie wordt verkregen, voorafgaand melding wordt gedaan aan het CvB. De FG houdt toezicht op het register voor de verwerkingsactiviteiten.

De FG wordt in staat gesteld taken uit te voeren en zijn deskundigheid in stand te houden en wordt, in lijn met artikel 38 AVG, voorzien van de benodigde middelen. De FG is adviseur van het CvB en rapporteert direct aan het CvB. De FG brengt jaarlijks een verslag uit over de bescherming van persoonsgegevens binnen de RUG, waaronder de stand van zaken met betrekking tot privacyvolwassenheid. Het verslag wordt beschikbaar gesteld aan het CvB en de Raad van Toezicht. Het verslag wordt ter informatie toegezonden aan de universiteitsraad.

De FG ondersteunt het CvB in het afleggen van verantwoording naar buiten toe, zowel aan toezichthouders als aan betrokkenen. De FG onderhoudt daarvoor contact met de toezichthoudende autoriteiten. De FG geeft aanbevelingen die strekken tot verdere optimalisering van de privacybeleidsvoering.

3.6.2. Verantwoordelijkheden en bevoegdheden IT-auditor

De interne IT-auditor monitort het risicomanagement en de effectiviteit van de risicomitigerende maatregelen ten aanzien van de universitaire processen en informatiesystemen. De IT-auditor van de RUG toetst in opdracht van het CvB of de FG de opzet, het bestaan en de werking van het universitaire privacybeleid en maatregelen die risico's voor de bescherming van persoonsgegevens mitigeren. De IT-auditor brengt deze werkzaamheden onder in een universitair auditplan. De IT-auditor brengt van diens werkzaamheden verslag uit aan de Commissie Privacy, Security en Informatiebeheer.

3.7. Verantwoordelijkheden en bevoegdheden Commissie Privacy, Security en Informatiebeheer

De Commissie Privacy, Security en Informatiebeheer adviseert het CvB over de ontwikkeling van universiteitsbreed beleid en werkprogramma's op het gebied van privacy, informatiebeveiliging en informatiebeheer. De commissie bewaakt dat privacy, informatiebeveiliging en informatiebeheer in lijn zijn met de strategische doelen van de universiteit. De commissie ziet toe op de toepassing van het eigenaarschapsmodel, waarmee verantwoordelijkheid voor processen, systemen, gegevens en risico's wordt bepaald. Wijzigingen in het privacybeleid worden te allen tijde voorgelegd aan deze commissie alvorens ze ter vaststelling aan het CvB worden aangeboden. De CISO en CPO rapporteren ieder kwartaal aan de commissie over de voortgang van de uitrol van hun werkprogramma's. De commissie bestaat uit een lid van het CvB (tevens voorzitter), een tweetal leden van het bedrijfsvoeringsberaad, een lid van het College van Decanen, de directeuren van University Services en het Centrum voor Informatietechnologie, de CISO en de CPO. De IT-auditor en de FG zijn adviserende leden.

3.8. Verantwoordelijkheden en bevoegdheden medezeggenschapsorganen

Voor zover dat vereist is op grond van de wet of intern beleid, worden de medezeggenschapsorganen van de RUG in staat gesteld hun bevoegdheden uit te oefenen ten aanzien van de wijze waarop de RUG uitvoering geeft aan de privacywet- en regelgeving. De bevoegdheden van de universiteitsraad op het gebied van privacy en bescherming van persoonsgegevens zijn vastgelegd in het Reglement Universiteitsraad.

4. Toepassing privacybeleid

4.1. Werkprogramma privacyvolwassenheid College van Bestuur, beleidsevaluatie, nader privacybeleid, protocollen

De RUG hanteert een gangbaar model voor het bepalen van de privacyvolwassenheid. Dit is het "Privacy Toetsingskader" van SURF.² De RUG heeft zich ten doel gesteld te acteren op minimaal een volwassenheidsniveau van gemiddeld 3.0 volgens dit model (op een schaal van 0-5). Bij het toepassen van het model wordt rekening gehouden met de structuur en cultuur

² Zie: <https://pec.surf.nl/surfaudit-toetsingskader-privacy/>.

van de organisatie. Het College van Bestuur stelt iedere twee jaar, in reactie op het beeld van het actuele universitaire volwassenheidsniveau, in een werkprogramma vast wat gedaan moet worden om het gewenste niveau te bereiken en te behouden. Het werkprogramma wordt door de CPO voorbereid in afstemming met het P&S-Gilde. De uitvoering ervan wordt door de CPO ondergebracht in de universitaire *Plan Do Check Act*-cyclus voor gegevensbescherming en de CPO bewaakt dat het werkprogramma wordt ingebed in de activiteiten van het P&S Gilde van faculteiten en diensten.

Onderhavig privacybeleid wordt minimaal een keer per twee jaar geëvalueerd en bijgewerkt. Het College van Bestuur stelt voor specifieke verwerkingen zo nodig nader privacybeleid vast.³ De Commissie Privacy, Security & Informatie stelt protocollen vast waarmee de uitvoering van de verplichtingen in de AVG wordt gefaciliteerd met een procesbeschrijving en werkinstructies. Deze protocollen worden uitgewerkt en beheerd door de CPO, waar nodig in samenwerking met de CISO.

4.2. PDCA-cyclus gegevensbeschermingfaculteiten en diensten

De faculteitsbesturen en de directies van de diensten zijn ervoor verantwoordelijk dat zij een *Plan Do Check Act*-cyclus implementeren waarmee zij het privacyvolwassen en compliant maken en houden van de processen binnen hun faculteit of dienst realiseren. In dat kader stellen zij vast hoe en wanneer het bestuur of de directie uitvoering geeft aan de in paragraaf 2.2 beschreven taken en verantwoordelijkheden. Zij doen dat door uitvoering te geven aan het risicomanagementbeleid en voortdurend privacyrisico's in kaart te brengen en te mitigeren met concrete acties en maatregelen ten aanzien van processen en systemen. Een en ander is nader beschreven in het protocol risico's en maatregelen P&S. De activiteiten van het bestuur of de directie worden jaarlijks beoordeeld door de FG, CPO, IT-auditor en de CISO van de universiteit. De inrichting en werking van de P&S-organisatie van de faculteit of dienst worden tevens beoordeeld. Het faculteitsbestuur of de directie ontvangt van de beoordeling een terugkoppeling.

4.3. Privacy by Design & by default, DPIA's

Innovatieve onderzoeksprojecten en nieuwe processen binnen de RUG, alsmede de systemen die deze processen ondersteunen, zijn zo opgezet dat de privacy-impact zo laag mogelijk is, terwijl de legitieme doeleinden van deze processen gerealiseerd worden. *Privacy by design* en *privacy by default* hebben een plek in het proces voor aanschaffen, ontwikkelen en implementeren van informatiesystemen. Privacy by design behelst het inbedden van de beginselen van de AVG in processen en systemen waarbinnen persoonsgegevens worden verwerkt, reeds in de ontwerpfase ervan. Privacy by Default behelst het zo afstellen van de standaardinstellingen van een systeem of proces dat de impact op de bescherming van de persoonlijke levenssfeer van de betrokkene zo beperkt mogelijk is.

Waar dat nodig is, wordt een *Data Protection Impact Assessment* uitgevoerd. De RUG heeft een protocol dat bepaalt wanneer dit verplicht is en dat het delen van inzichten uit de DPIA's

³ Denk bijvoorbeeld aan het beleid cameratoezicht.

stimuleert. Het protocol sluit minimaal aan bij de eisen van de privacywet- en regelgeving en regelt wanneer een ondersteunende rol van AJZ vereist is. Faculteitsbesturen en directies van diensten zijn verantwoordelijk voor de naleving van dit protocol. Wanneer een DPIA is uitgevoerd, wordt dit geregistreerd in het register als bedoeld in paragraaf 3.5. Een DPIA wordt te allen tijde gedeeld met de FG van de RUG ten behoeve van het verkrijgen van advies.

4.4. Gedragscodes en certificeringen

De RUG conformeert zich waar mogelijk en redelijk aan gedragscodes en certificeringseisen die een zorgvuldige en behoorlijke omgang met persoonsgegevens bevorderen. Het CvB besluit in het tweejaarlijkse werkprogramma aan welke gedragscodes de RUG zich conformeert. De FG kan de RUG adviseren zich te conformeren aan gedragscodes.

4.5. Register voor de verwerkingsactiviteiten

Alle verwerkingen van persoonsgegevens door of namens de RUG, worden geregistreerd in een centraal, openbaar beschikbaar, register⁴ dat wordt beheerd door de CPO. Dit register voldoet aan de eisen van de privacywet- en regelgeving, maar is daarnaast een instrument om privacyvolwassenheid te realiseren en daarover verantwoording af te kunnen leggen. De CPO zorgt, in samenspraak met de FG, ervoor dat het register hiervoor gebruikt kan worden en stelt de te registreren informatie vast. Het register is geschikt voor alle verwerkingen die de RUG uitvoert, zowel in de hoedanigheid van verantwoordelijke als van verwerker in de zin van de privacywet- en regelgeving. De CPO beoordeelt de geregistreerde verwerkingen en voorziet de faculteiten en diensten van advies over de risico's die bij een verwerking spelen.

4.6. Informatiebeveiliging

Het informatiebeveiligingsbeleid van de RUG en de daaronder hangende baseline met maatregelen, voorziet in een passende beveiliging van persoonsgegevens tegen onrechtmatige verwerking en onbevoegde toegang. De maatregelen kunnen technisch of organisatorisch zijn. Het informatiebeveiligingsbeleid is van toepassing op iedere verwerking van persoonsgegevens door de RUG, al dan niet met inzet van externe partijen (verwerkers) of gezamenlijk met een andere verantwoordelijke. Persoonsgegevens zijn ten minste geclassificeerd als 'vertrouwelijk' in de zin van het informatiebeveiligingsbeleid. Per proces waarbinnen persoonsgegevens worden verwerkt, wordt beoordeeld of dit niveau passend is. Faculteitsbesturen en directies van diensten zijn hiervoor verantwoordelijk.

4.7. Privacy-incidenten, datalekken

(Vermoedelijke) datalekken en andere (beveiligings)incidenten waardoor inbreuk wordt gemaakt op de bescherming van persoonsgegevens kunnen worden gemeld bij een daarvoor ingericht *meldpunt datalekken* waarvoor de CPO verantwoordelijk is. De meldingen worden behandeld volgens het Protocol meldplicht datalekken van de RUG. Het protocol wordt

⁴ Zie: <https://www.rug.nl/about-ug/policy-and-strategy/privacy-and-security-at-the-ug/processing-register/>.

jaarlijks geëvalueerd door de CPO, de CISO en de FG. Gemelde datalekken worden geregistreerd in een niet-openbaar register.

4.8. Verwerking van persoonsgegevens van de RUG door of samen met derden

De RUG kan de verwerking van persoonsgegevens uitbesteden aan derden, samen met derden verrichten of de persoonsgegevens aan derden verstrekken. AJZ ondersteunt bij het beoordelen van de rechtmatigheid van dergelijke activiteiten. Als de verwerking door een derde doorgang vindt, worden met deze partij schriftelijke afspraken gemaakt die ervoor zorgen dat een zorgvuldige en behoorlijke omgang met persoonsgegevens gewaarborgd is. De afspraken voldoen aan de eisen van de privacywet- en regelgeving, waaronder artikel 26 en 28 van de AVG.

4.9. Doorgifte van persoonsgegevens naar buiten de EER

Het verwerken van persoonsgegevens buiten de Europese Economische Ruimte (EER) is uitsluitend mogelijk indien passende waarborgen zijn getroffen voor de bescherming van de persoonsgegevens volgens de privacywet- en regelgeving. Voorafgaand aan een dergelijke verwerking, zal altijd de FG of AJZ aanwijzingen geven voor het treffen van deze waarborgen.

4.10. Transparantie en rekenschap

4.10.1. Privacyverklaring

Betrokkenen worden volledig, tijdig en in begrijpelijke taal geïnformeerd over de verwerking van hun persoonsgegevens door de RUG. Er is een RUG-brede privacyverklaring waar de betrokkene op wordt gewezen voorafgaand aan de verwerking van zijn persoonsgegevens. Deze wordt beheerd door de CPO.

Betrokkenen dienen voor specifieke verwerkingen waar nodig een specifieke privacyverklaring voorgelegd te krijgen, die de RUG-brede privacyverklaring aanvult en daarnaar verwijst. Het faculteitsbestuur en de directies van de diensten zijn ervoor verantwoordelijk dat deze specifieke privacyverklaring wordt opgesteld en voorgelegd. Zij stemmen dit af met de betrokken privacy- en securitycoördinator. Dit gebeurt bij wetenschappelijk onderzoek in afstemming met de ethische commissie. Een dergelijke aanvullende privacyverklaring wordt in ieder geval opgesteld wanneer de gegevens worden verwerkt op basis van toestemming van de betrokkene. Aanvullende privacyverklaringen worden geregistreerd bij AJZ.

4.10.2. Rechten van de betrokkene

Alle verzoeken, vragen en klachten van een betrokkene met betrekking tot de verwerking van zijn persoonsgegevens door de RUG, worden tijdig, zorgvuldig en behoorlijk beoordeeld en afgehandeld. Hiervoor is een *Centraal Loket Privacy* ingericht bij AJZ. Er is een protocol voor de afhandeling van de verzoeken die binnenkomen bij het loket. Hierin wordt beschreven hoe wordt omgegaan met verzoeken van betrokkene op grond van de privacywet- en regelgeving (bijvoorbeeld een inzageverzoek of een verzoek tot verwijdering van diens

persoonsgegevens). De CPO beheert dit protocol. Een betrokkene wordt in iedere privacyverklaring geïnformeerd over diens rechten en over het Centraal loket privacy.

4.10.3. Verantwoording aan privacytoezichthouders

De FG is op grond van de AVG contactpersoon voor de Autoriteit Persoonsgegevens. Dit laat onverlet dat het CvB verantwoording aflegt aan de bevoegde nationale en internationale privacytoezichthouders en de Raad van Toezicht. Het CvB is verantwoordelijk voor het verstrekken van de volledige informatie en het inzichtelijk maken van de privacyvolwassenheid van de RUG.

4.11. Communicatie en PR

Alle medewerkers worden geïnformeerd over dit privacybeleid en de taken en verantwoordelijkheden die zij op grond daarvan hebben. Hiertoe is een webpagina ingericht op het intranet van de RUG. De website wordt gevuld met informatie over de privacywet- en regelgeving en werkinstructies.. De RUG maakt daarnaast op de publieke website informatie openbaar over de omgang met persoonsgegevens en de privacy-visie van de universiteit. De informatie wordt opgesteld en onderhouden door de afdeling Communicatie van de dienst University Services van de RUG, in samenwerking met AJZ.

In het geval van een privacy-incident of andere mogelijke privacy-gerelateerde PR-issues, legt het CvB verantwoording af aan betrokkenen, toezichthouders en andere stakeholders. De FG kan, altijd in overleg met het CvB, verantwoording afleggen namens het CvB.

4.12. Bewustwording en training

De RUG werkt voortdurend aan bewustwording op het gebied van privacyvolwassenheid. Alle medewerkers van de RUG volgen een training waarmee zij op de hoogte worden gebracht van de relevante onderdelen van de privacywet- en regelgeving en werkinstructies voor de zorgvuldige omgang met persoonsgegevens.

4.13. Aard van dit privacybeleid

Dit privacybeleid geeft algemene richtlijnen voor het realiseren van privacyvolwassenheid, maar beschrijft niet de voorwaarden die kunnen gelden voor een specifieke verwerkingsactiviteit. Voor iedere verwerkingsactiviteit dient bewust en separaat onderzocht te worden hoe deze in overeenstemming wordt gebracht met wet- en regelgeving en dit beleid. Dit wordt zo nodig verankerd in nader privacybeleid.

5. Protocollen en nader privacybeleid

Dit algemene privacybeleid wordt verder uitgediept in protocollen en nader privacybeleid. De protocollen beschrijven werkprocessen met taken, verantwoordelijkheden en bevoegdheden voor de behandeling van datalekken, privacyverzoeken, DPIA's en P&S-risico's. Nader privacybeleid beschrijft de doelen, verantwoordelijkheden en nadere zorgvuldigheidsnormen voor specifieke verwerkingen met hoge risico's voor de bescherming van persoonsgegevens, zoals het cameratoezicht. Deze documenten zorgen ervoor dat de uitvoering van de

verplichtingen in de AVG goed is belegd binnen de organisatie. Het College van Bestuur heeft de volgende protocollen en het volgende nadere privacybeleid vastgesteld:

Protocollen	Nader privacybeleid
Protocol meldplicht datalekken	Beleid P&S Risicomanagement (tevens onderdeel van het informatiebeveiligingsbeleid van de RUG, vastgesteld 2024)
Protocol DPIA's en protocol DPIA in Research	Beleid Cameratoezicht (vastgesteld 2025)
Protocol Centraal loket privacy	Beleidsplan Domein Studenten en Onderwijs: beleid en richtlijnen voor de zorgvuldige verwerking van persoonsgegevens (vastgesteld 2020)