PLATFORM
INTEGRALE VEILIGHEID
HOGER ONDERWIJS

Een initiatief van de Vereniging Hogescholen en VSNU

KPMG

HANDREIKING

Definitieve versie, maart 2021

Handreiking voor het versterken van de privacygovernance bij HO-instellingen

Deze Handreiking is opgesteld in afstemming met het Platform Integrale Veiligheid Hoger Onderwijs (IV-HO)[1] en geeft adviezen over het verder versterken van de privacygovernance bij onderwijsinstellingen.

Achtergrond en doel van deze handreiking

Privacy en cybersecurity worden de afgelopen jaren gezien als belangrijke thema's[2] in de ontwikkeling van het veiligheidsbeleid en het crisismanagement van hogescholen en universiteiten. Het creëren van een veilige digitale leer- en werkomgeving die bestendig is tegen inbreuken en waar zorgvuldig met persoonsgegevens wordt omgegaan is een uitdaging waarmee alle onderwijs- en onderzoeksinstellingen te maken hebben. In het Covid-19-tijdperk is deze veilige digitale omgeving zelfs een onmisbare randvoorwaarde voor de integriteit en continuïteit van de primaire onderwijs- en onderzoeksprocessen.

"Voer een intrinsieke discussie in het CvB om de kernwaarden, de rol en de maatschappelijke positie van de onderwijsinstelling in het privacydebat te bepalen."

Corien Prins (hoogleraar Recht & Informatisering,
Tilburg University & voorzitter WRR)

---

[1] Opgesteld door KPMG op [01-12-2020] in samenwerking met de werkgroep privacygovernance van het Platform IV-HO. Wij bedanken hoogleraar Corien Prins (Tilburg University) en Ton Groot Zwaaftink (Voorzitter CvB Thomas More Hogeschool) en de bestuurders uit de Stuurgroep van het platform IV-HO: Marcel Nollen (Vrije Universiteit), Jet de Ranitz (SURF) en Jan Bogerd (Hogeschool Utrecht) voor hun input en feedback. Deze handreiking is overigens niet bedoeld als weergave van hun standpunten. Tevens hebben FG's van verschillende hoger onderwijsinstellingen conceptversies van feedback kunnen voorzien. Dit paper is een uitwerking van het thema Privacy uit het eerdere Postion Paper over de governance van Cybersecurity, Privacy en Kennisveiligheid dat door IV-HO is uitgebracht.

[2] In het 'Dreigingsbeeld Hoger Onderwijs 2018' worden de ontwikkelingen op het gebied van privacy en cybersecurity genoemd als de belangrijkste dreiging die invloed heeft op de veiligheid en het crisismanagement van hogescholen en universiteiten. Deze dreiging bestaat onder andere uit het risico op privacy-incidenten, zoals datalekken en het onrechtmatig gebruik van persoonsgegevens. Daarnaast krijgt het onderwerp volop aandacht in de media door de invoering en naleving van de vanaf mei 2018 gehandhaafde Europese privacywet, de Algemene Verordening Gegevensbescherming (AVG).

Om een veilige omgeving voor onderwijs en onderzoek onder verantwoordelijkheid van het College van Bestuur (hierna: 'CvB') te waarborgen, is een sterke privacygovernance essentieel. Deze handreiking biedt praktische adviezen over hoe u uw privacygovernance kunt versterken en daarmee de privacybescherming naar een hoger plan kunt tillen.

Het belang van een sterke privacygovernance in het hoger onderwijs

Bij het houden van grip op veilig onderwijs en onderzoek spelen privacy-ethische dilemma's een prominente rol. Privacy is daarmee dus niet enkel een compliancevraagstuk ('voldoen we hiermee compleet aan de AVG'), maar vergt tevens invulling vanuit ethisch oogpunt ('wettelijk mag het, maar moeten we dit wel willen?') en vanuit het oogpunt van risicoafweging ('het is vanuit de AVG gezien een hoog risico, maar we vinden het onderwijs- en risicotechnisch toch acceptabel het toe te staan').

Daarnaast heeft privacybescherming niet louter betrekking op de intern verwerkte persoonsgegevens, maar ook op de wijze waarop er in de gehele keten van samenwerkingspartners mee wordt omgegaan, met inbegrip van de platformen en systemen waarvan uw instelling afhankelijk is – ook afkomstig van partijen van buiten de EU. Dit betekent dat u als bestuurder bij de uitrol van nieuwe werkwijzen of platformen een maatschappelijke zorgplicht heeft de privacy van uw studenten, docenten, onderzoekers, onderzoeksdeelnemers en andere betrokkenen te bewaken. Vanwege deze afhankelijkheden en raakvlakken is het voor u als bestuurder behulpzaam om privacy niet in isolement, maar juist in samenhang met andere disciplines uit het veiligheidsrisicomanagement te behandelen. De inrichting van een sterke privacygovernance helpt u met het nemen van eigenaarschap voor privacy[3] dat naast het beheersen van AVG-vraagstukken bijdraagt aan het nemen van maatschappelijke verantwoording voor privacy door het CvB.

Waaraan dient de inrichting van een effectieve privacygovernance te voldoen?

Het is van belang te realiseren dat het CvB, als hoogste verantwoordelijke orgaan van de instelling, de wettelijke eindverantwoordelijkheid draagt voor privacy en aansprakelijk is wanneer de AVG structureel niet goed wordt nageleefd. Om als bestuurder deze verantwoordelijkheid te kunnen dragen en de juiste juridische en ethische afwegingen te kunnen maken, bent u doorgaans afhankelijk en gebaat bij advies van een sterk team van privacy-professionals binnen uw instelling. Uw interne privacyorganisatie vormt daarom de basis van de privacygovernance en ondersteunt u bij het maken van de juiste afwegingen, geschikte kaders voor de instelling te bepalen, privacybeleid op te stellen en deze krachtig te communiceren en te borgen, onder andere met AVG-/privacytraining. In de praktijk betekent dit de strategische positionering van privacyfuncties in alle geledingen van de organisatie, die samen een sterk samenwerkingsverband vormen. Deze privacyfuncties werken samen met andere disciplines op het gebied van integrale veiligheid, zoals informatiebeveiliging.

Een effectieve privacygovernance stelt uw instelling in staat om tijdig te anticiperen op ernstige datalekken, zoals van gevoelige onderzoeksgegevens of SIS-gegevens. Hierdoor voorkomt of beperkt u allereerst de privacyschade voor de betrokkenen, maar voorkomt u ook operationele, financiële of reputatieschade voor uw instelling door negatieve media-aandacht en/of optreden van Autoriteit Persoonsgegevens (hierna: 'AP') of de Inspectie van het Onderwijs. Daarnaast zorgt een goed ingerichte privacygovernance ervoor dat alle lagen van uw instelling doordrongen zijn van de privacy-visie van het CvB waardoor privacy-onvriendelijke werkwijzen of initiatieven worden voorkomen (privacy by design) en/of op tijd worden gesignaleerd. Tevens brengt een sterke privacygovernance u in een comfortabele privacypositie zodat u onder tijdsdruk cruciale privacykeuzes kunt maken en deze keuzes ook intern en extern kunt uitleggen. Op deze wijze bent u als bestuurder in staat om tot een gedegen en integrale besluitvorming te komen door risico's te analyseren, beleid en prioriteiten te bepalen, de juiste maatregelen te treffen en deze na een jaarlijkse evaluatie zo nodig bij te stellen.

[3] Logischerwijs betekent het nemen van eigenaarschap en maatschappelijke verantwoording door het CvB ook het vrijmaken van (financiële) middelen en fte's.

Hoe faciliteert het CvB de privacygovernance?

Een effectieve privacygovernance wordt door het CvB bereikt door het nemen en invullen van het eigenaarschap van privacy met uitstraling naar de gehele instelling, naar externe partners, zoals onderzoeksconsortia en subsidieverstrekkers, en naar de maatschappij. Belangrijk voor dit eigenaarschap zijn het voeren en uitdragen van haar privacybeleid, met welke commerciële binnen- en buitenlandse partijen de instelling wil samenwerken en welke grenzen worden gesteld aan het gebruiken en delen van persoonsgegevens. Om te zorgen dat privacy niet alleen bij het bestuur, management en de privacyfuncties leeft, maar bij alle faculteiten, diensten en externe partners hoog op de agenda staat moet het CvB het privacybeleid actief uitdragen en erop toezien dat de juiste maatregelen zijn geïmplementeerd, alsmede door privacy een vast onderdeel van de Planning- & Control-cyclus te laten uitmaken. Bovendien zou privacy onderdeel moeten uitmaken van het onderwijscurriculum.

Periodiek overleg tussen FG en CvB zorgt ervoor dat er continue aandacht voor privacy is. Hiermee blijft uw privacygovernance duurzaam en houdt u grip op de persoonsgegevens die binnen en buiten uw instelling worden verwerkt.

Hoe invulling te geven aan de Functionaris voor de Gegevensbescherming (FG) functie?

De belangrijkste strategisch adviseur van het CvB voor privacy is de FG. De FG heeft een wettelijk bepaalde onafhankelijke positie en houdt toezicht op de correcte toepassing en naleving van de AVG. De FG fungeert daarmee als eerste aanspreekpunt voor de AP. Op grond van de AVG zijn (vrijwel) alle onderwijs- en onderzoeksinstellingen verplicht om een FG aan te stellen. In het kader van *Good Governance* is het van belang de rol en taken van de FG in uw bestuursreglement op te nemen.

De FG wijst het CvB op haar privacyverantwoordelijkheden en het nemen van eigenaarschap. Daarom dient de FG een rechtstreekse rapportage- en escalatielijn met het CvB en indien nodig de Raad van Toezicht (hierna: 'RvT') te hebben. Deze rapportagelijn is essentieel: de FG wijst het CvB op privacyrisico's en -ontwikkelingen, helpt de prioriteiten te bepalen en het privacybeleid of -maatregelen bij te stellen om privacyverantwoord te kunnen besluiten en opereren. Tenslotte is de FG naast RvT en CvB de enige die op grond van de AVG gemandateerd is om zelf audits uit te voeren of om een interne of externe auditdienst te verzoeken een privacy-audit uit te voeren.

De FG bekleedt een functie waar kritieke of tegengestelde belangen mee gemoeid zijn. De organisatiebelangen kunnen conflicteren met het waarborgen van de privacy, hetgeen kan uitmonden in complexe kwesties, zoals bij het benutten van online studentgegevens en learning analytics voor het verhogen van het studierendement. De FG dient daarom gepositioneerd te worden in de 3e lijn van het *three lines (of defence)* risicomanagementmodel. De FG-functie valt niet te combineren met proces-, IT-, gegevens- of beveiligingsverantwoordelijkheden, zoals de CIO- of CISO-functie. Bij kleine of middelgrote instellingen laat de wet de ruimte om te kiezen voor een 'gezamenlijke' FG. De aanstelling van één FG voor meerdere onderwijsinstellingen van vergelijkbaar formaat bevordert daarnaast de onderlinge deling en uitwisseling van kennis en hulpmiddelen.

Wie voert het privacybeleid van de instelling uit voor het CvB?

De lijnorganisatie is verantwoordelijk (1e lijn) voor de uitvoering van het privacybeleid en voor het gepaste operationele gebruik van persoonsgegevens. Het is daarom noodzakelijk dat het CvB personen aanstelt die opvolging geven aan de beslissingen van het CvB: de Centrale Privacy Officer (hierna: 'CPO') en de Privacy Officer (hierna: 'PO')[4].

De CPO is de spin in het web die helpt om privacyrisico's naar een acceptabel niveau te reduceren en dient gepositioneerd te worden in de 2e lijn. De CPO voert het meest complexe privacywerk uit en staat in nauw

[4] Ook wel Privacycoördinator genoemd.

contact met de FG. Om te weten wat zich in de haarvaten van de instelling afspeelt, dient de CPO over aanspreekpunten in de organisatie te beschikken. Deze functie wordt ingevuld door de PO. De PO-functie draagt bij aan het opbouwen van een intern privacynetwerk, het verankeren van privacybeleid en ondersteunt de instelling met privacyvraagstukken rondom afdeling- of ketenspecifieke verwerkingen. De PO mag gepositioneerd zijn in alle lagen van de lijnorganisatie en is te combineren met verschillende rollen, bijvoorbeeld met integrale veiligheidsrollen of datasteward. Zo kan de PO voeling houden met relevante ontwikkelingen in het onderwijs, onderzoek en de bedrijfsvoering.

Het aantal fte's dat nodig is om de CPO- of PO-functie uit te voeren is sterk afhankelijk van de aard en omvang van de onderwijs- of onderzoeksinstelling. Een kleine of middelgrote instelling is wellicht gebaat bij één (deeltijd-) CPO, terwijl een grotere instelling gebaat kan zijn bij een fulltime CPO die meerdere PO's onder zich heeft, die zich elk richten op hun eigen focusgebied/domein.

Met de navolgende adviezen kunt u uw privacygovernance verbeteren en kunt u aantonen dat het vertrouwen van de samenleving in privacybescherming in het hoger onderwijs gerechtvaardigd is.

Welke aanbevelingen leiden tot een succesvol ingerichte privacygovernance?

- Het CvB dient zich bewust te zijn van haar eindverantwoordelijkheid om de bescherming van persoonsgegevens te waarborgen. Dit kunt u doen door eigenaarschap te tonen door duidelijke koers en kernwaarden rondom privacy op te stellen en uit te dragen en privacy te integreren in een meerjarenplan om het gewenste privacyvolwassenheidsniveau te bereiken én te borgen.
- Richt een periodieke rapportagelijn in van de FG aan het CvB (minimaal ieder kwartaal) en de RvT (minimaal jaarlijks) en zorg dat de FG – indien nodig ongevraagd – een formele ingang heeft bij bestuurlijk overleg.
- Draag zorg voor rolvastheid, zodat de FG vrij kan monitoren en adviseren en niet in initiatieven of (neven)functies wordt gezogen die niet stroken met zijn of haar onafhankelijke positie.
- Maak, in overleg met de FG, bewuste keuzes in de structurering van het privacyteam en het aantal (part-time) CPO's en PO's in dit team. Rust de FG en CPO daarnaast uit met mandaat, budget, scholing en capaciteit om de beleids- en jaarplandoelen (& audits) te kunnen bereiken en de privacybelangen zichtbaar te kunnen verdedigen.
- Organiseer een sectorbreed samenwerkingsverband van FG's, CPO's en PO's om kennisdeling en de uitwisseling van informatie en personeel te bevorderen en privacy-initiatieven, zoals het inkopen van producten of diensten, het afsluiten van gezamenlijke verwerkersovereenkomsten en het gezamenlijk uitvoeren van DPIA's voor sectorspecifieke diensten en verwerkingsprocessen te bevorderen.
- Pas het SURFaudit- en privacy-normen-&toetsingskader sectorbreed toe, en evalueer en verbeter dit kader jaarlijks. Dit kader helpt om vast te stellen of uw instelling voldoet aan de AVG en het helpt om het privacyvolwassenheidsniveau te bepalen dat past bij de aard en omvang van uw instelling. Voorts helpt het u om het geschikte ambitieniveau voor specifieke onderwijs- en onderzoeksprocessen of organisatieonderdelen te bepalen en op die wijze te monitoren op verbeteringen. Tegen dit privacykader kan dan ook periodieke interne of externe toetsing van de operationele werking van de getroffen privacymaatregelen plaatsvinden.
- Faciliteer als instelling en als gehele sector (incl. DUO, SURF en Studielink) dat studenten, onderzoekers en medewerkers actief regie op hun eigen persoonsgegevens kunnen uitoefenen, mede vanuit het oogpunt van Leven Lang Leren/Ontwikkelen. Hierbij kan dan naast online inzage ook digitale mogelijkheden tot aanvullingen, correcties, archivering, overdracht (o.a. minors, micro-credentials) en gedifferentieerde toestemming voor externe verstrekking op een gestandaardiseerde en veilige wijze worden aangeboden.