Hogeschool van Amsterdam

JAARVERSLAG FG

2018

Functionaris voor Gegevensbescherming
2018

JAARVERSLAG FG

2018

AUTEUR
Martijn de Hamer

AFDELING
Functionaris voor Gegevensbescherming

DATUM
24 april 2019

VERSIE
1.0

Samenvatting

De Hogeschool van Amsterdam hecht grote waarde aan de bescherming van de persoonsgegevens van haar betrokkenen. Door verantwoord om te gaan met de gegevens van haar medewerkers, studenten, alumni en prospecten, geeft de organisatie de ruimte om te kunnen experimenteren, fouten te maken, te leren van deze fouten en te excelleren. De juiste omgang met persoonsgegevens zorgt voor de atmosfeer die randvoorwaardelijk is om talent maximaal te kunnen ontplooien. Deze zorg voor de privacy van haar betrokkenen sluit daarmee aan bij de geactualiseerde missie en visie van de HvA. [1]

In februari 2018 is de HvA gestart met de projectmatige implementatie van de AVG. Voor die tijd was er in diverse diensten en afdelingen al gestart met stappen om te voldoen aan de aankomende wetgeving. Er zijn vanaf de start grote stappen gezet om zicht en grip te krijgen op de verwerkingen binnen de organisatie. In dit jaarverslag beschrijft de Functionaris voor Gegevensbescherming de ontwikkelingen, gebeurtenissen en trends op het gebied van privacy, zowel binnen als buiten – zij het met gevolgen voor – de organisatie. Als onderdeel van de taken van de FG wordt in deze rapportage ook aandacht geschonken aan de rechten van de betrokkenen en de plichten van de organisatie onder de verordening. Hierbij wordt geconstateerd dat het aantal datalekken dat gemeld is bij de FG en vervolgens conform procedure afgehandeld, is gegroeid – een indicatie van een groeiend privacy-bewustzijn – en dat het aantal verzoeken door betrokkenen om hun rechten uit te oefenen beperkt is gebleven.

[1] https://visie.mijnhva.nl/Documents/De%20geactualiseerde%20Missie_Visie_HvA-juli2018.pdf

Inhoudsopgave

1. Inleiding

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht geworden en daardoor moeten organisaties zich houden aan specifieker en explicieter geformuleerde wet- en regelgeving op het gebied van privacy. Naast de explicieter geformuleerde rechten van de betrokkenen en de steviger plichten van de verwerkingsverantwoordelijken, heeft de toezichthouder ook sterkere middelen gekregen om naleving van de wet te handhaven. De FG heeft dit jaarverslag terugkijkend naar 2018 geschreven vanuit zijn eigen perspectief. Het doel van het document is om de stand van zaken met betrekking tot privacy toe te lichten. Hiernaast geeft het inzicht in de mate waarin de HvA voldoet aan de geldende wetgeving en haar eigen *Privacybeleid en beleid verwerking persoonsgegevens* en *Privacywaarden*.

2. Activiteiten Toezichthouder

In de laatste maanden van 2018 is de Autoriteit Persoonsgegevens als toezichthouder hard aan het groeien en neemt ze stappen die erop duiden dat ze haar positie steviger aan het innemen is. Allereerst is ze het personeel aan het zoeken en aannemen om de voorgenomen groei te kunnen realiseren. Hiernaast wordt er meer duidelijk over haar rol en de manier waarop ze deze invult. Zo heeft ze het UWV een last onder dwangsom opgelegd tot het moment dat er voldoende beveiligingsmaatregelen getroffen zijn om de gezondheidsgegevens van haar betrokkenen afdoende te kunnen beschermen.[2] De Nederlandse tak van Uber heeft een boete gekregen van 600.000,-- euro vanwege een te laat gemeld datalek.[3] De Nationale Politie riskeert een dwangsom als zij niet – na herhaalde berichten – per begin februari haar persoonsgegevens beter afschermt voor de interne organisatie.[4] Tot slot is de Belastingdienst gedwongen een investering te doen om zijn werkwijze aan te passen omdat ze per 1 januari 2020 niet meer het BSN van zelfstandigen mogen gebruiken als BTW nummer.[5]

Naast deze toegenomen activiteit is de last op de AP ook toegenomen door het aantal datalekken dat in 2018 is gemeld. Ten opzichte van 2017 is dit aantal meer dan verdubbeld.[6] Helaas ontbreken de cijfers om te staven of deze groei ook te herkennen binnen de HvA.
De toezichthouder heeft aandacht voor de onderwijssector en publiceert met enige regelmaat artikelen en adviezen die hierop betrekking op hebben.[7]. Hiernaast zijn er vanuit diverse kanten geluiden te

[2] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-dwingt-uwv-met-sanctie-gegevens-beter-te-beveiligen
[3] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-legt-uber-boete-op-voor-te-laat-melden-datalek
[4] https://autoriteitpersoonsgegevens.nl/nl/nieuws/nationale-politie-beschermt-politiegegevens-nog-steeds-niet-goed-genoeg
[5] https://autoriteitpersoonsgegevens.nl/nl/nieuws/belastingdienst-mag-bsn-niet-meer-gebruiken-btw-identificatienummer
[6] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/jaarrapportage_meldplicht_datalekken_2018.pdf
[7] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-roept-scholen-op-zorgvuldig-om-te-gaan-met-beeldmateriaal-van-leerlingen
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/01_onderzoeksrapport_boor.pdf
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_wijziging_aanpassingswet_studiefinanciering_bes.pdf

horen, dat de toezichthouder meer aandacht krijgt voor het hoger onderwijs. De Hogeschool van Amsterdam (HvA) heeft dit op een aantal momenten en verschillende manieren zelf ondervonden. De toezichthouder heeft ook stellige en voor de HvA relevante posities ingenomen met betrekking tot concepten als WiFi-tracking, Internet of Things devices en cameratoezicht.[8] Verwerkingen van dit soort vertegenwoordigen een hoog risico voor de betrokkenen en mogen daarom alleen onder strikte voorwaarden.

In de nabije toekomst zal de ePrivacy verordening worden aangenomen. Twee jaar hierna zal deze van kracht worden. Hiermee zullen ook de bepalingen uit de telecommunicatiewet worden veranderd en zal er – ter vervanging van de huidige telecomwet – een uitvoeringswet verschijnen. Gelet op het uitgangspunt van consistentie in de nieuwe verordening, zal de taak om hierop toezicht te houden zeer waarschijnlijk ook komen te liggen bij de Autoriteit Persoonsgegevens. Gezien een recente uiting lijkt ze zich hier op voor te bereiden.[9]

3. Media

In de media wordt aan de lopende band geschreven over incidenten waarbij persoonsgegevens zijn betrokken. Het gaat hierbij regelmatig om grote organisaties die veel data – en daardoor ook persoonsgegevens – verwerken. Deze organisaties moeten voldoen aan de nodige wet- en regelgeving en moeten daarom de informatiebeveiliging op orde hebben. Toch gaat dit regelmatig mis. Zo is bij British Airways de data – inclusief creditcardgegevens – van 380.000 klanten gestolen.[10] Bij Albert Heijn zijn de logingegevens van circa 10.000 klanten gelekt door een programmeerfout en RTL heeft publiek gemaakt, dat er persoonlijke gegevens van tienduizenden RTL-accounts zijn gelekt.[11] [12]
Dit type datalekken vraagt om extra zorg voor de betrokkenen en het voorkomen dat ze gebeuren bij de HvA vraagt doorlopende aandacht van de organisatie.

4. Ontwikkelingen inzake AVG

Diverse artikelen van de AVG zjin voor meerderlei uitleg vatbaar. Jurisprudentie zorgt daarbij voor meer helderheid. Uitspraken in rechtszaken en nadere toelichting door de toezichthouder geven een steeds beter beeld over hoe te handelen binnen de AVG.
Zo is er in 2018 meer helderheid gegeven over inzageverzoeken door betrokkenen, zij het onder de Wbp, en hoe deze te behandelen onder de AVG.[13] Hiernaast is door de Autoriteit Persoonsgegevens meer helderheid gegeven aan de HvA over de interpretatie van één van de gronden waarin in specifieke gevallen het verbod op de verwerking van bijzondere persoonsgegevens door scholen wordt

[8] https://autoriteitpersoonsgegevens.nl/nl/nieuws/bedrijven-mogen-mensen-alleen-bij-hoge-uitzondering-met-wifitracking-volgen
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp260rev01_nl.docx
https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-inzicht-gebruik-camera%E2%80%99s-voor-beveiligen-eigendom
[9] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_ap_cookiewalls.pdf
[10] https://www.britishairways.com/en-gb/information/incident/data-theft/latest-information
[11] https://www.nu.nl/internet/5562599/tienduizend-wachtwoorden-van-albert-heijn-klanten-gelekt.html
[12] https://www.rtlnieuws.nl/tech/artikel/4500196/datalek-rtl-nederland-videoland
[13] https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHSHE:2018:363

opgeheven.[14] De Advocaat Generaal van het Europeese Hof van Justitie heeft een uitspraak gedaan over het gebruik van de Facebook “like” knop op de website van een organisatie.[15] Zodra een organisatie een dergelijke knop op haar website plaatst, wordt deze mede verwerkingsverantwoordelijke en heeft zich daarmee te houden aan de bijbehorende plichten.

5. Ontwikkelingen bij HvA

5.1 Implementatie AVG

Om de Algemene Verordening Gegevensbescherming (AVG) te kunnen toepassen op de verwerking van persoonsgegevens binnen de HvA, is in 2018 een project gestart om de eerste belangrijke stappen richting compliance te zetten. De gedelegeerd opdrachtgever is het hoofd Juridische Zaken en twee projectleiders hebben de taak om de activiteiten binnen het project uit te voeren. De drie activiteiten waaraan de meeste prioriteit zijn gegeven, zijn: het vullen van het verwerkingenregister,[16] de verwerkersovereenkomsten met derde partijen ondertekend en op orde krijgen en het bewustzijn voor het onderwerp verbeteren. Tijdens de audit op de implementatie van de AVG binnen de HvA (zie de paragraaf: *Audit op implementatievermogen AVG*) is duidelijk geworden dat dit register nog onvoldoende is gevuld en dat er onvoldoende prioriteit aan is gegeven.
De stuurgroep-leden vertegenwoordigen belangrijke stakeholders uit de organisatie. De projectgroep bestaat uit de informatiemanagers voor de faculteiten en diensten, die de rol van privacy contactpersoon (PCP) hebben gekregen – tot het moment dat deze rol een formelere status heeft gekregen. De FG heeft geen rol in het project en is als toehoorder aanwezig bij de project- en stuurgroepoverleggen.

5.2 Privacybeleid

Ten tijde van de inwerkingtreding van de AVG, is het privacybeleid van de HvA vastgesteld door het College van Bestuur.[17] Dit beleid is binnen het implementatietraject opgesteld als wettelijke verplichting en geeft richting aan de manier waarop met privacy wordt omgegaan binnen de organisatie.[18] Dit document beschrijft de verantwoordelijkheden voor de verschillende aspecten van privacy en legt vast welke plichten iedere persoon die persoonsgegevens verwerkt, heeft. Het geeft de organisatie ook de mogelijkheid om personen aan te spreken op een eventuele onverantwoordelijke verwerking van persoonsgegevens.

5.3 Autorisatiebeleid

Ter verbetering van de bescherming van persoonsgegevens, is het belangrijk om te weten wie bij welke data moet kunnen. Omdat er nog geen beleid bestaat waarin wordt vastgelegd hoe wordt omgegaan met autorisaties, kan niet op naleving worden gestuurd. De CISO heeft in samenspraak met de FG van de HvA en de FG van de UvA een eerste opzet gemaakt voor het autorisatiebeleid, dat breed door de organisatie moet gaan worden nageleefd.

---

[14] In uAVG, artikel 30, lid 2 onder a. wordt gesproken over scholen en leerlingen. De AP heeft toegelicht, dat deze regel ook geld voor hogescholen en studenten.
[15] https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-12/cp180206nl.pdf
[16] Zoals verplicht in AVG artikel 30.
[17] https://beleid.mijnhva.nl/nl/BeleidsdocumentenMWSTU/privacybeleid-en-beleid-verwerking-persoonsgegevens.pdf
[18] AVG, artikel 24, lid 2

5.4 Privacywaarden

Het project heeft als onderdeel van de implementatie van de AVG een beschrijving van de privacy-waarden opgesteld en gepubliceerd op zowel het privacy-lemma voor studenten als dat voor medewerkers.[19] Deze beschrijving is breed gedragen door de stuurgroep van het project en toont de toewijding van de organisatie voor het onderwerp. Hiernaast schept het een kader bij besluiten over verwerkingen.

5.5 Functionaris voor Gegevensbescherming

Na het vertrek van de Functionaris voor Gegevensbescherming (FG), die onder het regime van de Wet Bescherming Persoonsgegevens zijn werk uitvoerde, is deze rol een korte tijd in een beperkt aantal uren ad-interim ingevuld door de Chief Information Security Officer (CISO). Per 1 september is de functie van FG weer volledig ingevuld. Tijdens de uitvoer van het project en tijdens de daarop volgende overdracht aan de staande organisatie, heeft de FG vanwege capaciteitsgebrek ook een deel van de taken waargenomen die horen bij een Chief Privacy Officer. Hierbij heeft hij steeds zijn verantwoordelijkheid moeten houden en een modus moeten zoeken om zijn rol zuiver te houden. De FG gaat zich in het nieuwe jaar meer terugtrekken uit de uitvoering en meer tijd besteden aan de taken die horen bij zijn rol.

De aanpak van de FG is er in de eerste periode vooral op gericht om de collega's te informeren over het belang van het onderwerp en ze te inspireren om hun manier van werk zo aan te passen, dat privacy-schendingen in het dagelijks werk worden beperkt. Hiernaast is een van de taken van de FG het verhogen van de bewustwording van de organisatie over de diverse aspecten die privacy raken. Hiervoor gebruikt hij per situatie het best passende middel, zoals een memo om een knelpunt te beschrijven of een presentatie om een groep collega's te informeren.

5.6 Afstemming tussen de HvA en de UvA

De HvA deelt vier diensten met de UvA. Voor de medewerkers die verantwoordelijk zijn voor de gezamenlijke HvA/UvA verwerking van persoonsgegevens binnen deze diensten is een afwijkend geluid van beide organisaties onwerkaar. Daarom is in de uitvoer van de implementatieprojecten van de beide organisaties met grote regelmaat afgestemd tussen de diverse rollen in het project. Ook de FG's van de HvA en de UvA stemmen continu hun activiteiten, adviezen en gesprekken met elkaar af. Hierbij is consistentie voor de gedeelde diensten niet de enige reden. De twee gelieerde organisaties moeten ook aan de buitenwereld, zoals bijvoorbeeld aan de Autoriteit Persoonsgegevens, een gelijkklinkend geluid laten horen. Een verschillende aanpak tussen twee, zo nauw gerelateerde organisaties kan duiden op een onzorgvuldige bescherming van de persoonsgegevens van de betrokkenen.

5.7 Privacy en security governance

De projectleden en projectleiders van het AVG project leveren veel inspanning om de verordening te implementeren bij de HvA door de grondbeginselen op orde te krijgen. Zodra deze infrastructuur er ligt blijft de aandacht voor het onderwerp noodzakelijk. Privacy zal vanaf het ontwerp onderdeel moeten zijn van elk nieuw project, systeem of beleid. Hiernaast zullen zaken als verbeterprojecten, de productie van handleidingen, het beantwoorden van vragen en het ontwikkelen van templates en gereedschappen voor de medewerkers capaciteit blijven vragen. De aard van de organisatie vraagt om een hybride privacy-organisatie waarbij specialisten beschikbaar zijn in zowel de centrale als de decentrale onderdelen.

[19] https://az.hva.nl/medewerkers/az-lemmas/medewerkers/hva-breed/juridische-zaken/avg/privacy.html

In afstemming met de UvA wordt in opdracht van de Chief Security Officer van de HvA gewerkt aan de structuur om deze privacy-organisatie te kunnen opzetten en in gezamenlijkheid met informatiebeveiliging en integrale veiligheid duurzaam en consistent te kunnen borgen. Hierbij wordt onder andere gekeken naar de gedeelde diensten, de samenhang en samenwerking tussen de drie veiligheidsgebieden en de bestaande rollen en capaciteit. In de structuur die wordt uitgewerkt, wordt zowel centrale als decentrale capaciteit beschreven en worden randvoorwaarden geschetst waaraan deze capaciteit moet voldoen.

5.8 Audit op implementatievermogen AVG

In het laatste kwartaal van 2018 is een audit naar de implementatie van de AVG binnen de HvA uitgevoerd. De uitkomst van deze audit geeft een beeld van de zaken die moeten worden veranderd bij de bestendiging van de onderwerpen privacy en informatiebeveiliging in de hierboven genoemde governance-structuur. Op basis van een gezamenlijke sessie met vertegenwoordigers uit de stuurgroep, de projectgroep, de projectleiders, de FG en de auditor zijn verbeterpunten en maatregelen besproken, beschreven en toegepast, voor drie probleemgebieden die zijn geïdentificeerd in het auditrapport.

5.9 Bewustzijn en kennis

Als onderdeel van het AVG implementatietraject is een reeks opleidingen gefaciliteerd waarmee de stakeholders de gelegenheid is geboden om basiskennis van de AVG op te doen en op die manier een gezamenlijk vocabulaire op te bouwen. Alle PCP's hebben de voor hun relevante sessies bijgewoond. Uit het niveau van de vragen die worden gesteld door de PCP's blijkt dat hun kennisniveau gestaag is gegroeid in de periode sinds de start van het project.
Binnen het project is ook, gezamenlijk met de UvA, een bewustwording-campagne gestart waarbij diverse onderwerpen met betrekking tot informatiebeveiliging en privacy onder de aandacht worden gebracht. De campagne is een terugkerend fenomeen voor een brede doelgroep waarbij vooral concrete handvatten worden gegeven. Hiernaast is een projectleider awareness aangesteld, met als opdracht om awareness als groter en overkoepelend thema uit te werken in een breed scala van activiteiten en tastbare producten. Ook in dit traject zullen informatiebeveiliging en privacy gezamenlijk onder de aandacht worden gebracht.

5.10 Onderzoek

Naast onderwijs en bedrijfsvoering heeft het onderwerp privacy ook de aandacht binnen de onderzoeken die worden uitgevoerd bij de HvA. Zo behandelen de datastewards van de diverse faculteiten dit onderwerp in hun periodieke overleg. De stafafdeling Onderwijs en Onderzoek is vertegenwoordigd in dit overleg en de FG houdt via dit gremium regelmatig contact met de ontwikkelingen op het gebied van onderzoek.
Het AVG implementatieproject heeft aanzienlijke inspanning geleverd om de belangen op het gebied van privacy in onderzoeken te borgen via de Ethische Commissie. De technische omgeving die de commissie als middel in gebruik gaat nemen krijgt een rol bij de borging van het onderwerp in nieuwe onderzoeken.

Zoals in hoofdstuk 2 is beschreven, heeft de toezichthouder bijzondere aandacht voor een aantal nieuwe technieken en ontwikkelingen. Omdat dit type technieken zeer relevant zijn voor toekomstige innovaties en de studenten, docenten en onderzoekers de juiste kennis hiervan nodig hebben om te kunnen bijdragen aan de toekomst, gebruikt de HvA ze op een aantal plekken. Zo wordt er onderzoek gedaan naar de werking en de toepasbaarheid van apparaten zoals slimme camera's en slimme

“microfoons” zoals de Google Home en de Amazon Alexa. De FG heeft bijzondere aandacht voor deze en andere ontwikkelingen.

5.11 Verhoogde aandacht voor privacy

Buiten de innovaties binnen de HvA die hierboven zijn beschreven, bestaat een aantal andere prominente aandachtsgebieden en ontwikkelingen waar privacy bijzondere aandacht behoeft en de FG deze in 2018 ook heeft gegeven. Het eerste onderwerp is Learning Analytics als bijproduct van het gebruik van de Digitale Leer Omgeving (DLO). Zowel studenten als docenten hebben een belang bij dit concept, omdat de gegevens hoe zij werken met het lesmateriaal veel inzichtgeeft in potentiele knelpunten. Omdat learning analytics een grote impact op de privacy van deze gebruikers kan hebben – immers, studenten en docenten worden potentieel gevolgd en in de gaten gehouden – is het van belang om het middel op een verantwoorde en goed doordachte manier in te zetten. De HvA is actief bezig om de visie en strategie met betrekking tot dit concept vorm te geven.

De door de overheid gestimuleerde beweging richting open research en open data is een ander onderwerp waar privacy bijzondere aandacht vraagt. Het kan op termijn voorkomen dat er persoonsgegevens gepubliceerd moet worden om onderzoeksresultaten te laten verifieren door derden. Dit kan een risico inhouden voor de betrokkenen van de HvA. De FG heeft hier bijzondere aandacht voor en zoekt hierbij ook aansluiting bij FG’s van andere kennisinstellingen.

Om de ontwikkeling van de organisatie te faciliteren en de groeiende hoeveelheid data te kunnen verwerken, wordt een project uitgevoerd met als doel de ingebruikname van Office 365. In oktober 2018 publiceerde Strategisch Leveranciersmanagement Microsoft Rijk, als onderdeel van het ministerie van Justitie en Veiligheid, het verslag van de Data Protection Impact Assessment die ze heeft laten uitvoeren om inzicht te krijgen in de risico’s die het gebruik van Office 365 met zich meebrengt.[20] De bevindingen in het document was aanleiding voor zowel de FG’ s van HvA en UvA als de CISO van beide organisaties om in een gesprek met de programmamanager en de directeur van ICTS de zorgen te addresseren. De FG is betrokken bij dit onderwerp.

Tot slot is er extra aandacht voor de privacy van de betrokkenen van de HvA bij het gebruik van tracking-technieken op de websites. Door gebruik van zogenaamde tracking-cookies en pixels van externe leveranciers kan de organisatie de bezoekers van haar websites volgen. Hierdoor krijgt de HvA inzicht in bijvoorbeeld de efficientie van het gebruik van specifieke marketing campagnes. Het gebruik van dergelijke technieken stelt deze bezoekers – waarvoor de HvA verantwoordelijk is[21] – ook bloot aan een potentieel risico. De persoonsgegevens van deze personen worden gedeeld met een derde partij die de gegevens voor haar eigen doelen kan gebruiken. Het staat buiten kijf dat deze verwerking in al haar aspecten binnen de wet moet gebeuren. Daarnaast moet de organisatie oog blijven houden voor de balans tussen efficientie en de groeiende negatieve toon rondom dit onderwerp, met het hieruit volgende risico op reputatieschade.

[20] https://www.rijksoverheid.nl/documenten/rapporten/2018/11/07/data-protection-impact-assessment-op-microsoft-office
[21] https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-12/cp180206nl.pdf

6. Incidenten

Een datalek is een inbreuk op de beveiliging, die heeft geleid of kan leiden tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van persoonsgegevens. Vanuit het perspectief van de huidige FG, t.w. in de periode van 1 september t/m 31 december 2018, zijn 17 incidenten met betrekking tot persoonsgegevens gemeld waarvoor de HvA verwerkingsverantwoordelijke is. Hierbij moet worden opgemerkt dat er binnen de organisatie nog veel onbekend is over het concept datalekken en dat vaak een voorval niet wordt herkend als een inbreuk in verband met persoonsgegevens. Het aantal datalekken dat is gemeld binnen de organisatie – en waarop kon worden gehandeld – is mogelijk geen realistische weergave van de werkelijkheid. Hieronder een overzicht van het aantal meldingen per maand:

Tabel 1 Datalekken per maand

Maand	# datalekken
September	1
Oktober	3
November	7
December	6

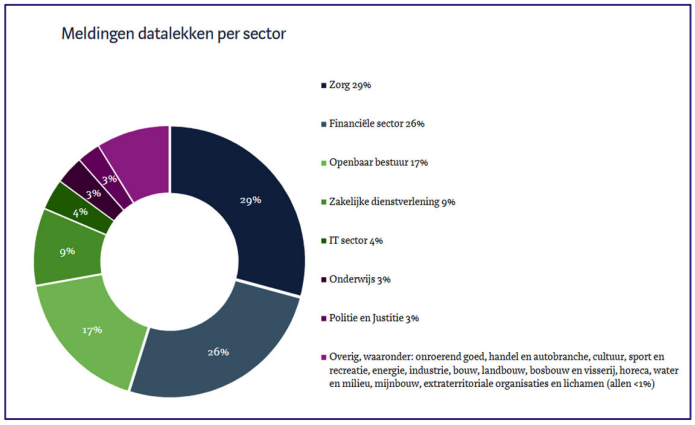
De toezichthouder verdeelt in haar meld-stramien en jaarrapportage de datalekken onder in een aantal categorieën.[22] Hieronder het overzicht van datalekken waarvoor HvA verwerkingsverantwoordelijke is, onderverdeeld in de categorieen, zoals in gebruik bij de AP.

Tabel 2 Datalekken Per categorie AP

Oorzaak	Aantal
Persoonsgegevens verstuurd of afgegeven aan een verkeerde ontvanger	3
Apparaat, gegevensdrager of papier kwijtgeraakt en/of gestolen	7
Brief of postpakket kwijtgeraakt of geopend retour ontvangen	0
Hacking, Malware en/of Phishing	1
Persoonsgegevens per ongeluk gepubliceerd	6
Persoonsgegevens van een verkeerde klant getoond in klantportaal	0
Persoonsgegevens nog aanwezig op afgedankt apparaat	0
Overig	0

22 https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/meldplicht_datalekken_halfjaarrapportage_q1_en_q2_2018_algemeen.pdf

De onderwijs-sector is verantwoordelijk voor 3% van de meldingen van datalekken bij de Autoriteit Persoonsgegevens. Dat zijn bijna 630 meldingen die gedaan zijn door onderwijsinstellingen. In deze percentages is de omvang van de sector niet meegewogen. Binnen de drie procent wordt niet nader gespecificeerd hoeveel meldingen er zijn gedaan door primair, secundair en tertair onderwijsinstellingen.



Figuur 1 Bron:Meldplicht Datalekken: Facts & Figures (AP)

In haar publicatie: Meldelicht datalekken: facts & figures; Overzicht feiten en cijfers 2018 schrijft de AP dat ze op de hoogte is van niet gemelde datalekken en dat ze dit “als een ernstige zaak” beschouwt.[23] Ze kondigt daarbij aan, dat ze zich hier in 2019 extra op zal focussen en dat de onderzoeken die daaruit vloeien mogelijk zullen leiden tot sancties.

In 2019 heeft de AP haar boetebeleidsregels aangepast om aan te sluiten bij de nieuwe privacywetgeving.[24] De basisboetes die daarin worden beschreven zijn fors. Hiernaast is een recidivetermijn gesteld van 5 jaar. De AP gaat uit van een verhoging van de boete met 50% in geval van recidive.

Naast de incidenten die hebben geleid tot een datalek waren er ook voorvallen waarbij geen persoonsgegevens zijn ingezien door derden of verloren zijn gegaan. Zo is er een aantal laptops en telefoons verloren geraakt die binnen een dag weer zijn geretourneerd. Daarnaast was tijdens de bezetting van het P.C. Hoofthuis in september 2018 de oorzaak van een potentieel datalek.[25] Tijdens deze bezetting is rekening gehouden dat de bezetters toegang zouden kunnen krijgen tot de systemen met hierop persoonsgegevens in het pand. Onderzoek door het CERT heeft uitgewezen dat de aanwezige systemen niet zijn gebruikt en de hierop aanwezige gegevens niet zijn ingezien, verwijderd of veranderd.

23 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/jaarrapportage_meldplicht_datalekken_2018.pdf, p. 2
24 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-past-boetebeleidsregels-aan
25 http://www.uva.nl/over-de-uva/organisatie/beleid-ondersteuning-medezeggenschap/centrale-ondernemingsraad/actueel/statement-centrale-ondernemingsraad-over-bezetting-p.c.-hoofthuis.html

7. Rechten van de betrokkenen

In de periode die deze rapportage beschrijft, is het aantal verzoeken van betrokkenen om hun rechten uit te oefenen beperkt. In de informatieuitingen met betrekking tot privacy is opgenomen dat inzage in en wijziging van eigen gegevens voor een groot deel mogelijk is in de daarvoor bestemde systemen.[26] [27] Mogelijk dat hierdoor het aantal verzoeken beperkt is gebleven.

Recht	# verzoeken
Inzage	2
Rectificatie	0
Gegevenswissing	1
Bepering van verwerking	0
Overdraagbaarheid	0
Bezwaar	0

8. Risico's en adviezen

8.1 Privacy

8.1.1 Inzicht in verwerkingen

In het rapport van de eerder genoemde audit naar de implementatie van de AVG binnen de HvA is beschreven dat de registratie van de verwerkingen zoals opgenomen in het verwerkingenregister – verplicht gesteld in artikel 30 van de AVG – nog van onvoldoende kwaliteit is. Vanwege de grootte van de organisatie en de beperkte tijd van de PCP's voor het onderwerp is het register ook onvolledig. Hierbij moet worden opgemerkt dat inzicht krijgen in en het beschrijven van de verwerkingen bij een organisatie met de omvang, de structuur en de dynamiek van de HvA nu eenmaal tijd kost. Het project besteedt veel tijd en aandacht aan de ondersteuning bij het verbeteren van de kwaliteit en de compleetheid van het register. Hierbij wordt gebruik gemaakt van zogenaamde invulsessies en hiervoor is de instructie voor de PCP's verbeterd op basis van de commentaren uit deze groep.
De FG is in grote mate afhankelijk van de kwaliteit en volledigheid van het register voor zijn toezichthoudende activiteiten. Hij zal pas zicht hebben op de meest risicovolle verwerkingen zodra er een beter inzicht in de verwerkingen mogelijk is. Hierom is het advies om in het najaar opnieuw een scan te laten doen van de volledigheid van het register en de kwaliteit waarmee de hierin opgenomen verwerkingen zijn beschreven.

[26] https://az.hva.nl/medewerkers/az-lemmas/medewerkers/hva-breed/juridische-zaken/avg/wat-zijn-mijn-rechten/wat-zijn-mijn-rechten.html
[27] https://az.hva.nl/studenten/az-lemmas/studenten/hva-breed/juridische-zaken/privacy/wat-zijn-mijn-rechten/wat-zijn-mijn-rechten.html

8.1.2 Bewustzijn

Een deel van de inbreuken in verband met persoonsgegevens is veroorzaakt door een gebrek aan bewustzijn van de risico's voor de betrokkenen. Door middel van de HvA en UvA-brede bewustzijnscampagne worden de hiaten in de algemene kennis opgevuld. Dit is een eerste stap om de medewerkers die persoonsgegevens verwerken te helpen om de risico' s in te kunnen schatten. Om het juiste kennisniveau te kunnen garanderen is continue aandacht nodig voor het onderwerp via een breed scala aan middelen. Aan het einde van 2018 is een programma gestart waarbinnen het bewustzijn over de onderwerpen informatiebeveiliging en privacy gezamenlijk onder verschillende doelgropen bij zowel HvA als UvA wordt verhoogd.
In de dagelijkse gang van zaken moeten medewerkers en studenten weten waar ze met hun vragen terecht kunnen. Hiervoor is een structuur werkend en in ontwikkeling, waarbij middels trainingen, risico-analyse sessies en overleggen met de PCP's vragen worden gehoord, besproken en beantwoord.

8.1.3 Inzicht in incidenten

Zoals is te lezen in het hoofdstuk *Incidenten* zijn alleen die inbreuken gemeld, die bekend zijn en waarvan de medewerker of student zich heeft gerealiseerd dat er zich een potentieel datalek heeft voorgedaan. Als onderdeel van de werkzaamheden in het kader van bewustzijn gaat de FG ook nadrukkelijk aandacht gegeven aan de verplichting die de organisatie heeft in het kader van datalekken. Aansluitend daarop is het bewustzijn rondom datalekken en het handelingsperspectief voor student en medewerker een speciaal punt van aandacht binnen het awareness programma (zie *Bewustzijn en kennis).*

8.1.4 Capaciteit

Er is een bepaalde, nader vast te stellen capaciteit nodig om de privacy van de betrokkenen binnen de HvA te kunnen garanderen. Hiervoor is kennis nodig van zowel privacy als informatiebeveiliging. In de periode na inwerkingtreding van de AVG hebben de FIM's de additionele taak gekregen om als contactpersoon voor het project op te treden en zo de nodige projectactiviteiten uit te (laten) voeren. Hiernaast heeft de FG ze in de laatste vier maanden van het jaar steeds vaker betrokken bij de afhandeling van het toenemende aantal meldingen van datalekken (zie daarvoor paragraaf Incidenten), waarvoor hun specifieke kennis vaak onmisbaar is. Voor een beperkte tijd is dit haalbaar. Echter, uit de audit naar het AVG project is gebleken dat prioriteit voor de activiteiten horende bij deze rol, hoewel hard nodig, niet gegarandeerd is. Ten tijde van schrijven wordt gewerkt aan een plan om deze capaciteit te borgen. In dit plan wordt uitgegaan van rollen met als primaire taak het uitvoeren van de activiteiten horende bij de twee vakgebieden. Gedurende het traject blijft de FG nauw betrokken bij de borging van het onderwerp in de organisatie.

8.2 Informatiebeveiliging

Informatiebeveiliging en privacy zijn intrinsiek afhankelijk van elkaar. De privacy van de betrokkenen binnen de HvA kan niet worden gegarandeerd zonder dat de informatiebeveiliging van de systemen waarop de persoonsgegevens worden verwerkt op orde is. De twee onderwerpen vragen daarom een gezamenlijke aanpak. Op het gebied van informatiebeveiliging is een aantal knelpunten te identificeren die een risico vormen voor de privacy van de betrokkenen van de HvA.
De CISO heeft in opdracht van de CvBs van de HvA en de UvA een programmaplan geschreven om de informatiebeveiliging binnen de instellingen te verbeteren. Dat wordt op dit moment uitgevoerd.
Om IB en privacy te stroomlijnen hebben de FG's en de CISO wekelijks overleg over incidenten, datalekken, kwetsbaarheden en risico's en hoe deze gezamenlijk goed kunnen worden aangepakt.

Daarnaast zal de FG ook nauw betrokken zijn bij de verbetering van de diverse processen rondom informatiebeveiliging.

8.2.1 Onderzoek- en responscapaciteit

Zodra er zich een ICT veiligheid-incident voordoet, zijn er in een belangrijk deel van de voorvallen persoonsgegevens in het geding. Om te onderzoeken wat de impact is voor de betrokkenen is het belangrijk dat een (ICT) inbreuk wordt onderzocht. Binnen de HvA bestaat een Computer Emergency Respons Team (CERT) dat als doel heeft respons te bieden in geval van incidenten en noodgevallen. Ten tijde van schrijven is de capaciteit van dit organisatieonderdeel onvoldoende om het noodzakelijke onderzoek te doen naar inbreuken in verband met persoonsgegevens. Het CERT registreert meldingen en stuurt deze door aan de FG ter verdere afhandeling. In dit proces is nog ruimte voor verbetering. Incidenten die bij de HvA spelen worden nu voor een groot deel afgehandeld door CERT-UvA.
De capaciteit – beschreven in kennisgebieden, rollen en verantwoordelijkheden – is onderdeel van het verbeterplan Informatiebeveiliging HvA zoals wordt uitgevoerd onder leiding van de CISO van de HvA en de UvA. Bij de doorontwikkeling van het CERT moet rekening worden gehouden met de activiteiten die raken aan incidenten in verband met persoonsgegevens.

8.2.2 Beveiliging ICT-middelen

Zoals te lezen is in de paragraaf *Incidenten,* is een groot deel van de incidenten veroorzaakt door onvoldoende beveiligde ICT-middelen. De middelen die worden uitgeleverd bieden onvoldoende weerstand zodra deze in verkeerde handen komen. In de privacy verordening wordt gesteld dat passende technische en organisatorische maatregelen ter bescherming van persoonsgegevens moeten worden getroffen.[28] In het geval van laptops en andere mobiele gegevensdragers heeft de toezichthouder duidelijk laten weten wat een passend niveau van beveiliging is. In haar communicatie in verband met een incident aan het einde van 2018 heeft ze expliciet geëist dat deze middelen versleuteld zijn zodra er persoonsgegevens op worden verwerkt. Zodra er bijzondere categorieën van persoonsgegevens worden verwerkt moet het systeem ook op afstand gewist kunnen worden.[29] Deze maatregelen ontbreken op een belangrijk deel van de systemen die in gebruik zijn bij de HvA.
Systemen die worden gebruikt om diensten aan te bieden – zoals webapplicaties en databases – zijn onvolledig in zicht. Zo is uit incidenten gebleken dat in niet alle gevallen bekend is wat voor gegevens er op de systemen aanwezig zijn en wat de stand van de beveiliging van het systeem is. Hieruit volgt dat veel gegevens niet worden verwijderd, dat de beveiligingsmaatregelen niet worden bijgehouden en dat inbreuken in verband met persoonsgegevens niet worden gezien of herkend.
Het is belangrijk om periodiek een controle uit te voeren naar de staat van de beveiliging van de systemen. Door dit te vergelijken met het voor het systeem passend beschermingsniveau wordt inzichtelijk wat er in de huidige situatie moet veranderen om dit niveau te halen.
Er loopt een aantal initiatieven door de CISO om de risico's op dit vlak nog meer inzichtelijk te maken en maatregelen te treffen om het risico te beperken. De CISO en de FG werken hierin nauw samen.

9. Vooruitkijkend

In overleg met de voorzitter van het CvB loopt het jaarplan van de FG voor 2019/2020 gelijk met het aankomende collegejaar. Terwijl het jaarplan wordt geschreven en afgestemd heeft de FG een aantal prioriteiten. Een deel hiervan – met name de prominente en risicovolle verwerkingen – is beschreven in

[28] AVG art. 32
[29] Bijzondere categorieën van persoonsgegevens, zie: AVG, art. 9

paragrafen *Activiteiten Toezichthouder* en *Verhoogde aandacht voor privacy*. Hiernaast blijven bewustwording, ontwikkelingen rondom open research en de bestendiging van de onderwerpen privacy en informatiebeveiliging binnen de HvA onderwerpen die een belangrijk deel van de agenda van de FG vullen.

10. Conclusie

De HvA heeft in 2018 veel bereikt op het gebied van privacy. De infrastructuur voor het opdoen en houden van inzicht in de verwerkingen van persoonsgegevens, met bijhorende risico's is gelegd en kan nu worden doorontwikkeld. Zo is de basis gelegd om als organisatie te kunnen doorgroeien naar het gewenste volwassenheidsniveau en de goede bescherming van de persoonsgegevens van de betrokkenen kunnen volhouden.

Er zijn drie punten van aandacht bij het laten doorleven van privacy en de bescherming van persoonsgegevens.

Allereerst heeft het onderwerp privacy een grote impuls gekregen in de aanloop naar de datum van inwerkingtreding van de AVG. De grote vordering die is gemaakt in 2018 toont aan dat aandacht voor het onderwerp werkt. Houd de aandacht voor privacy en laat deze niet verwateren als het in de directe omgeving minder vaak besproken wordt of het minder vaak de media haalt.

Een tweede punt van aandacht is de inspanning die moet worden gedaan om privacy gemeengoed te maken. De verantwoorde en veilige omgang met persoonsgegevens vergt bewustzijn en kennis. Elke student en medewerker moet weten wat hij hiervoor moet doen in zijn dagelijkse activiteiten. Dat is nog niet het geval. Naast de voortdurende aandacht die nodig is, hebben de mensen – en dus de organisatie –hulp nodig. Zorg dat ze die krijgen door voldoende capaciteit hiervoor beschikbaar te maken. De volwassenheid van de privacy-organisatie blijft alleen op peil wanneer hier blijvende zorg voor is en inspanning voor wordt geleverd.

Tot slot is de verwevenheid van informatiebeveiliging en privacy van groot belang. Om de bescherming van de persoonsgegevens binnen de HvA te kunnen garanderen moeten naast de organisatorische ook de technische maatregelen op orde worden gebracht en gehouden. De ambitie van de organisatie om informatiebeveiliging door te ontwikkelen naar volwassenheidsniveau 3 is van groot belang.[30] Hierbij is het noodzakelijk om niet alleen het gewenste volwassenheidniveau te halen, maar dit ook vast te houden. Dit vergt – net als het geval is bij privacy – blijvende aandacht en inspanning.

[30] cf. *Programmaplan Verbetering Informatiebeveiliging*