Hogeschool van Amsterdam

JAARVERSLAG FG 2019

In controle zijn

Functionaris voor Gegevensbescherming
2019

JAARVERSLAG FG 2019

In controle zijn

AUTEUR
Martijn de Hamer

AFDELING
Functionaris voor Gegevensbescherming

DATUM
4 maart 2020

VERSIE
1.0

Inhoudsopgave

Inhoudsopgave **3**

1. Inleiding **5**

2. Leeswijzer **6**

3. Jaarverslag **6**

4. Vooruitkijkend **8**

5. Conclusie **9**

6. Bijlage: Activiteiten Toezichthouder **10**
6.1 Ontwikkelingen 10
6.2 Uitdaging 10
6.3 Helder standpunt 11
6.4 Boetes en schadevergoedingen 11

7. Bijlage: Media **13**
7.1 Techbedrijven 13
7.2 Datalekken 14

8. Bijlage: Ontwikkelingen inzake AVG **15**
8.1 Jurisprudentie 15
8.1.1 Inzageverzoek en examenvragen 15
8.1.2 Cookie Consent 15
8.2 Richtlijnen uit de EU 15
8.3 Aanpalende wet- en regelgeving 16
8.3.1 Selectielijst Hogescholen 16
8.3.2 Archiefwet 17
8.4 De VS als verwerkingslocatie 17

9. Bijlage: Ontwikkelingen bij HvA **17**
9.1 Realisatie jaarplan FG 17
9.2 Informatiebeveiliging 17
9.3 Autorisatiebeleid 18
9.4 Administratie 18
9.4.1 Verwerkingenregister 20
9.4.2 Verwerkers / verwerkersovereenkomsten / gegevensuitwisselingsovereenkomsten 20
9.4.3 DPIA's 21
9.5 Implementatie AVG 21
9.6 Privacy en security governance 22
9.7 Organisatie brede verwerkingen 23
9.7.1 Algemeen 23
9.7.2 MS Office 365 23

9.7.3 MS Intune 24
9.7.4 Logging en Monitoring 24
9.7.5 Onderwijsdata-analyse 25
9.8 IoT apparaten 25
9.9 Bewaartermijnen 26
9.10 Betrokkenheid FG 26
9.11 Periodiek meten 27
9.12 Audit op implementatievermogen AVG 28
9.13 Cookies 28
9.14 Communicatie en bewustwording 28
9.15 Onderzoek 29
9.16 Verbinding 29

10. Bijlage: Incidenten 30
10.1 Algemeen 30
10.2 Vermissingen 30
10.3 Mandaat 31
10.4 Datalekkenregister 31
10.5 Datalekken 31

11. Bijlage: Rechten van de betrokkenen, klachten en bezwaren 34

12. Bijlage: Risico's en adviezen 34
12.1 Algemeen 34
12.2 Governance 34
12.3 Informatiebeveiliging 35
12.3.1 Onderzoek- en responscapaciteit 35
12.3.2 Basisprocessen 35
12.3.3 Schaduw-ICT 36
12.4 Administratie 36
12.5 Bewustzijn 36
12.6 RDM 36
12.7 Richtlijn betrekken FG 37
12.8 Samenvatting risico's en adviezen: 37

1. Inleiding

De FG heeft een aantal taken en één daarvan is om bij te dragen aan een cultuur waarin zorgvuldig wordt omgegaan met persoonsgegevens. Het spreekt voor zich dat de organisatie zich moet houden aan haar eigen privacy beleid, de Algemene Verordening Persoonsgegevens en andere relevante wetgeving, waarin wordt gesproken over tot de persoon herleidbare gegevens. Bij het uitvoeren van zijn werk heeft de FG altijd de zorg voor de betrokkene voorop staan. Zaken als onbewust omgaan met persoonsgegevens, onvoldoende beveiligde systemen en een incompleet inzicht in waar en hoe persoonsgegevens worden verwerkt binnen de organisatie kunnen leiden tot grote risico's voor medewerkers en studenten. In dit jaarverslag wordt de ontwikkeling beschreven die de organisatie op verschillende vlakken met betrekking tot privacy heeft doorgemaakt in het jaar 2019 en welke ontwikkelingen buiten de HvA een effect kunnen hebben hierop. Uit de voorbeelden volgt concluderend welke drie gebieden op dit moment het meeste kunnen bijdragen aan de betere bescherming van persoonsgegevens binnen de HvA en daarmee aan de zorg voor onze studenten en medewerkers.

Het thema van dit jaarverslag is *In controle zijn* en dit is niet voor niets gekozen. In artikel 5 van de Algemene Verordening Gegevensbescherming worden de beginselen van elke verwerking van persoonsgegevens beschreven. Deze kunnen alleen worden ingevuld als de organisatie grip op haar gegevens heeft en dat is alleen mogelijk als wordt voldaan aan een aantal voorwaarden. De meest voor de hand liggende zijn de volgende. De organisatie moet inzicht hebben in de gegevens die worden verwerkt en deze moeten zijn vastgelegd in een register. Hierin moet ook staan waar de gegevens vandaan komen – hoe krijgt de HvA deze – en waar ze naartoe gaan – aan wie verstrekt de HvA ze. Voor de gegevens die we aan organisaties verstrekken moeten overeenkomsten worden afgesloten, de zogenaamde verwerkersovereenkomsten. De technische en organisatorische maatregelen moeten op orde zijn en worden geadministreerd.

Vervolgens, om ervoor te zorgen dat de organisatie in controle is, moeten mensen de juiste dingen doen. Deze mensen moeten worden benoemd en geschoold. De organisatie moet op veel plaatsen nog leren dat er serieus naar deze mensen moet worden geluisterd. Welke mensen welke rollen en verantwoordelijkheden hebben en hoe deze mensen werken ten opzichte van elkaar moet zijn vastgelegd in een governance.

In de anderhalf jaar na inwerkingtreding van de AVG heeft de HvA veel voortgang geboekt bij de bescherming van persoonsgegevens. De eerste stappen zijn gezet in 2018 en 2019 heeft in het teken gestaan van de voorbereiding van een grote stap voor de organisatie. Er is hard gewerkt om een structuur te bouwen en verankeren binnen de HvA, waarin is vastgelegd hoe privacy, informatiebeveiliging en fysieke veiligheid gezamenlijk verder worden gebracht. Starten met werken volgens deze structuur zal de risico's, zoals beschreven in *Bijlage: Risico's en adviezen* wegnemen of beperken.

Het jaarverslag FG 2019 bestrijkt het kalenderjaar 2019 en loopt daarmee dakpansgewijs met het jaarplan van de FG, dat op verzoek van het College van Bestuur gelijkloopt met het collegejaar. Dit heeft enerzijds tot gevolg dat er kan worden teruggekeken op de uitvoering van een deel van het jaarplan, terwijl vooruitkijkend de plannen voor het komende half jaar kunnen worden bijgesteld.

2. Leeswijzer

In dit verslag wordt van buiten naar binnen gekeken en is bewust kort gehouden. De onderbouwing voor het verslag is te vinden in een reeks bijlagen. Deze kennen dezelfde opbouw als het verslag over 2018. Allereerst worden de relevante activiteiten en prioriteiten van de Autoriteit Persoonsgegevens in 2019 beschreven. Daarna volgt in *Bijlage: Media* een kleine terugblik op grote ontwikkelingen die in de internationale media te lezen zijn geweest. Eén onderdeel hiervan is een inzicht in welke grote datalekken hebben plaatsgevonden en welke sancties hiervoor zijn opgelegd. In *Bijlage: Ontwikkelingen inzake AVG* wordt de nadere duiding van de AVG door zowel de Autoriteit Persoonsgegevens als de European Data Protection Board (EDPB) beschreven. Deze informatie geeft de HvA meer duidelijkheid over hoe ze moet omgaan met persoonsgegevens. *Bijlage: Ontwikkelingen bij HvA* beschrijft wat de HvA heeft gedaan om privacy binnen de organisatie te verhogen en in *Bijlage: Incidenten* is beschreven hoeveel en welk type datalekken de organisatie heeft meegemaakt. Belangrijke regels in de privacy verordening gaan over de rechten van de betrokkenen. De verzoeken tot uitoefening hiervan staan beschreven in *Bijlage: Rechten van de betrokkenen, klachten en bezwaren*. De risico's met bijbehorende adviezen die de FG geeft op onderstaande bevindingen staan beschreven in *Bijlage: Risico's en adviezen*.

3. Jaarverslag

Het jaarverslag FG 2019 weerspiegelt de ontwikkelingen en uitdagingen waarvoor de HvA afgelopen jaar heeft gestaan. De organisatie is in 2019 hard bezig geweest om te leren werken met de privacy verordening en te wennen aan de extra aandacht die moet worden gegeven aan de verwerking van persoonsgegevens. In 2019 is de voorbereiding gedaan om in 2020 grip te kunnen krijgen op privacy en in 2021 in controle te kunnen komen.

In het afgelopen jaar heeft de Autoriteit Persoonsgegevens (AP) veel werk verricht. Denk hierbij aan activiteiten om het bewustzijn en de kennis over specifieke onderwerpen bij organisaties te verhogen. Als toezichthouder voor een nieuwe verordening en met een bewegend spelveld, heeft ze het erg druk en dit is merkbaar. Diverse geluiden – onder andere van de AP zelf – maken duidelijk dat ze meer werk hebben dan ze aankunnen. Er blijven vragen en klachten onbeantwoord en dit leidt tot speculatie over hun slagkracht.

Niet alleen bij de AP is veel gebeurd op het gebied van privacy. Alle organisaties die een aanwezigheid in Europa hebben moeten voldoen aan de AVG. Daarom is er in de media veel gepubliceerd over dit onderwerp. In 2019 een terugkerend thema te herkennen in het groeiende besef van de verwerking van persoonsgegevens door grote technologie bedrijven. Organisaties die digitale diensten aanbieden – zij het betaald of onbetaald – verwerken meer gegevens over hun gebruikers dan alleen datgene wat de gebruiker bewust deelt. De doelen waarvoor de gegevens worden verwerkt zijn ook met nevelen omhuld, met als gevolg dat gebruikers – onder andere binnen organisaties – de controle uit handen hebben gegeven aan bijvoorbeeld Google en Amazon. In de media is een aantal prominente datalekken beschreven. Hiernaast heeft een aantal Europese toezichthouders heeft in 2019 de eerste boetes uitgedeeld onder de AVG en in Nederland heeft de AP haar eerste AVG boete opgelegd aan het HagaZiekenhuis. De toedracht is vaak van dien aard, dat dit in ook bij de HvA had kunnen gebeuren en het is goed dat de organisatie hieruit de lessen leert.

Europa leert omgaan met de nieuwe privacy verordening. Er zijn diverse ontwikkelingen geweest inzake de AVG, die relevant zijn voor de HvA. Naast twee rechterlijke uitspraken die helpen om de verordening beter toe te passen, zijn ook de voortgang van en plannen met andere wetgeving relevant. Verder is er grote twijfel uitgesproken door het Hof van Justitie van de Europese Unie, over de adequaatheid van het VS Privacy Shield als maatregel voor de bescherming van persoonsgegevens van ingezetenen in de EU bij verwerkingen door partijen in de VS. Dit vertegenwoordigen geen snelle en acute veranderingen. Het zijn ontwikkelingen waar de organisatie komend jaar en waarschijnlijk daarna mee te maken krijgt.

De HvA zelf heeft veel gedaan in de aanpak om de persoonsgegevens van haar betrokkenen te beschermen. Eén van de zaken die in begin 2020 een grote stap vooruit moet betekenen is het vaststellen van de governance met betrekking tot veiligheid en het inrichten van de privacy-governance. In 2019 is veel tijd besteed aan de voorbereidingen voor dit besluit en de bijbehorende investering. De investering geldt voor bedrijfsvoering, onderwijs en onderzoek, waarbij de potentiele risico's bij de laatste groter zijn vanwege de aard van de gegevens die daarbij worden verwerkt en de nog onvoldoende capaciteit om deze goed te beschermen. Waar vorig jaar is gewerkt om zo goed als mogelijk de basis op orde krijgen, kan in 2020 worden gewerkt om grip te krijgen op privacy. Het is de ambitie om privacy in 2021 te hebben opgenomen in de organisatie brede PDCA cyclus.
De inzet van de HvA om goed om te gaan met privacy wordt op een aantal vlakken duidelijk. Voor in ieder geval twee organisatie brede verwerkingen is een grote investering in zowel tijd als geld gedaan. De implementatie van Office 365 heeft vertraging opgelopen omdat eind 2018 door de Rijksoverheid bekend is gemaakt dat er hoge risico's waren verbonden aan het gebruik ervan. Deze risico's zijn inmiddels beperkt tot een acceptabel niveau. Hiernaast is serieus gewerkt aan de kaders waarbinnen onderwijsdata-analyse kan worden gedaan op basis van gegevens uit de Digitale Leer Omgeving. De aanpak, het belang en het doel van deze verwerking is met een groep van diverse belanghebbenden onderzocht. Hierbij is de aansluiting gezocht met andere instellingen die ook met dit vraagstuk bezig zijn. Tot het moment dat deze strategie is vastgesteld door het College van Bestuur wordt er nog geen analyse gedaan op basis van onderwijsdata.

De HvA is een innovatieve kennisinstelling waarvoor technologische ontwikkelingen relevant zijn. Nieuwe technologieën – zoals het gebruik van Internet of Things (IoT) apparaten en algoritmen – leveren nieuwe mogelijkheden, maar ook privacy uitdagingen op. Omdat dit veld nog erg onvolwassen is, de risico's nog onbekend zijn en de mogelijkheden onbeperkt lijken, moet de organisatie bij elke voorgenomen verwerking zorgvuldig te werk gaan. Het is niet voor niets een van de onderwerpen waar de toezichthouder in de komende drie jaar extra aandacht voor heeft.

Inbreuken met betrekking tot persoonsgegevens – datalekken – komen in alle organisaties voor en ze hebben een diversiteit aan oorzaken. Het aantal datalekken dat de FG in 2019 heeft ontvangen is **51**. Dit is net zoveel als het jaar ervoor, als het aantal meldingen van de laatste vier maanden van 2018 wordt doorgetrokken naar een heel jaar. Hiermee wijkt de HvA af van de landelijke lijn. De AP heeft in 2019 een algemene toename in meldingen van 29% gezien. De onderwijs sector heeft ten opzichte van 2018 een groei van 1% laten zien en is verantwoordelijk geweest voor 4% van de meldingen bij de AP in 2019. De FG heeft onvoldoende inzicht in en wordt onvoldoende betrokken bij de incidenten waar de HvA een formele plicht heeft met betrekking tot persoonsgegevens. Hierdoor komt de HvA bij veel incidenten haar plichten niet na.

De HvA is transparant over welke persoonsgegevens ze verwerkt, is duidelijk in haar communicatie en geeft haar betrokkenen controle over hun eigen gegevens. Mogelijk is hierdoor het aantal verzoeken tot uitoefenen van de rechten door betrokkenen beperkt geweest. Er zijn twee gegronde inzageverzoeken geweest en was er slechts één verzoek tot verwijdering. Hiernaast is er één formeel bezwaar tegen een verwerking geweest. Dit is door het decentrale onderdeel dat verantwoordelijk is voor de verwerking afgehandeld.

De drie grootste oorzaken waardoor de organisatie een risico loopt zijn de volgende: Allereerst is het uitblijven van een besluit over de voorgenomen governance – algemeen en specifiek over privacy – in 2019 een beperkende factor geweest. Omdat mensen die hier decentraal een rol in hebben niet zijn benoemd tot privacy officer, zijn alle inspanningen om de bescherming van persoonsgegevens te bevorderen vrijblijvend en naar beste kunnen uitgevoerd. Ten tweede, gekoppeld met de nodige structuur, is de achterstand die de organisatie loopt met het op orde brengen van de administratie. De basis is in 2019 gelegd. In 2020 moet worden gewerkt om grip te krijgen op de gegevens die worden verwerkt, om in 2021 in control te kunnen zijn. De grip op gegevens wordt versterkt door een goed inzicht te hebben in de verwerkingen van persoonsgegevens, te weten welke risico's de betrokkenen lopen en hoe deze worden beperkt. Tot slot is de staat van de informatiebeveiliging een risico voor de privacy binnen de HvA. De grootte, de complexiteit en de innovatieve kracht van de organisatie vraagt een gedegen aanpak op dit vlak. Hierbij horen de nodige capaciteit, kennis en middelen. In 2019 is de verbetering in beweging gezet. In 2020 moet deze worden voortgezet en bestendigd.

4. Vooruitkijkend

Het jaarplan van de FG 2019/2020 loopt gelijk met het hogeschooljaar. Hierin staan de prioriteiten van de FG, zoals vastgesteld op het moment van schrijven. Gedurende het jaar hebben ontwikkelingen zowel binnen als buiten de HvA een verschuiving in deze prioriteiten veroorzaakt. Zie hiervoor onder andere paragraaf *Ontwikkelingen toezichthouder* (6.1) en *Onderwijsdata-analyse* (9.7.5). Bewustwording, ontwikkelingen rondom onderzoek en de bestendiging van de onderwerpen privacy en informatiebeveiliging binnen de HvA blijven de aandacht van de FG houden.

Hiernaast is een aantal aankomende ontwikkelingen relevant voor de HvA. In 2020 zijn als minder acute bewegingen de aanpassingen in wet- en regelgeving te verwachten. De ePrivacy Verordening (ePV) heeft potentieel gevolgen voor de manier waarop de HvA zal moeten omgaan met cookies en het al dan niet volgen van websitebezoekers. Mocht Privacy Shield, net als de Safe-Harbor uitgangspunten, door de EU niet meer als geldig worden gezien, dan moet de organisatie heroverwegen welke gegevens worden verstrekt aan partners in de VS. Een soortgelijke situatie bestaat met betrekking tot verstrekkingen van persoonsgegevens aan het Verenigd Koninkrijk. Als de EU op 31 december 2020 geen adequaatheidsbesluit heeft genomen over de bescherming in de recent vertrokken EU-lidstaat, moeten andere en strengere overeenkomsten worden afgesloten met leveranciers in dit land. Anders dan de discussie over Privacy Shield kent de HvA de termijn waarbinnen ze zich moet voorbereiden.

Tot slot gaat de versnelling in de digitale transformatie met zekerheid gevolgen opleveren voor de bescherming van persoonsgegevens. De toename in het gebruik van gegevens door de hele organisatie heen – van onderzoek tot bedrijfsvoering – en de verschuiving van het type gegevens – de groei van het aantal IoT systemen – hebben gevolgen voor de hoeveelheid gevoelige gegevens,

waaronder de bewegingen en beelden van personen. Het is belangrijk dat de HvA aan het begin van elk project of initiatief de aspecten rondom informatiebeveiliging en privacy meeweegt.

De basis voor een goede bescherming van persoonsgegevens is gelegd in 2019. In 2020 werkt de HvA om grip op haar gegevens te krijgen en in 2021 moet ze doorgroeien naar het volgende volwassenheidsniveau, om daarmee in control te komen.

5. Conclusie

In 2019 is voorgezet wat in 2018 is gestart. Er wordt op steeds meer plaatsen bekend dat er zorgvuldig gehandeld moet worden bij een verwerking van persoonsgegevens. Op basis van diverse awareness bijeenkomsten en activiteiten is te concluderen, dat dit bewustzijn nog niet vanzelf aanwezig is bij de medewerkers en dat is ook zo te verwachten. In gesprekken over privacy wordt vaak het vergelijk met autogordels aangehaald. Toen in 1975 het gebruik van de autogordel verplicht werd, heeft het jaren geduurd voor mensen het vanzelfsprekend vonden om een gordel te dragen. Gewenning heeft er voor gezorgd dat nu de eerste actie bij instappen is om de gordel te willen pakken. Zo zal dit ook moeten groeien met het werken volgens de AVG.

De basis die in 2018 is gelegd is in 2019 zoveel verstevigd, dat het jaar 2020 kan worden gebruikt om grip te krijgen op de gegevens. Hiervoor moeten drie punten die hierboven zijn genoemd prioriteit krijgen, t.w. governance, administratie en informatiebeveiliging. De HvA is nog niet in controle. Als deze drie zaken op orde zijn, ligt er een solide basis om de organisatie in controle te brengen.

6. Bijlage: Activiteiten Toezichthouder

6.1 Ontwikkelingen

Vlak voor en direct na de inwerkingtreding van de Algemene Verordening Gegevensbescherming, heeft de Autoriteit Persoonsgegevens (AP) een grote personeelswissel meegemaakt. Gedurende het jaar 2019 is er stevig gewerkt aan de werving van nieuwe medewerkers. Tegelijkertijd heeft ze veel werk gestopt in haar profilering als toezichthouder op de naleving van deze nieuwe verordening. Daarvoor heeft ze heeft gedurende het jaar over een aantal onderwerpen documenten gepubliceerd die organisaties in Nederland moeten helpen bij het goed toepassen van de AVG en de uAVG. Zo heeft ze achtereenvolgens campagnes gehouden over de onderwerpen “Wat betekent de privacywet voor jou(w bedrijf)?”, datalekken, verwerkers van persoonsgegevens, persoonsgegevens van zieke medewerkers en grondslagen.

Verder krijgt ze de middelen om haar taak in 2020 steviger uit te oefenen. De minister voor Rechtsbescherming heeft in een brief aan de kamer toegelicht dat de AP in 2019 meer nadruk heeft gelegd op handhaving en sanctieoplegging.[1] De verwachting is dat de AP dit in 2020 doorzet. In die zelfde brief schrijft de minister dat de toezichthouder jaarlijks 3,4 miljoen euro extra krijgt – bovenop de structurele verhoging van 7 miljoen voor de jaren 2019 en verder. In november 2019 heeft de AP haar prioriteiten en strategie voor de jaren 2020 tot en met 2013 gepresenteerd. [2]

Aandacht AP voor activiteiten HvA:
De AP heeft aangekondigd dat ze de komende jaren – van 2020 tot en met 2023 – in haar toezichtwerk extra nadruk gaat leggen op drie aandachtsgebieden, te weten: datahandel, digitale overheid en Artificiële Intelligentie. Hiermee probeert ze de (onterechte) signalen dat privacywetgeving nieuwe ontwikkelingen in de weg staat te adresseren en het groeiende digitale onrecht dat nu voorkomt tegen te gaan. Omdat onder deze prioriteiten ook zaken vallen als Internet of Things, profilering en Smart Cities zijn ze alle drie relevant voor de HvA in haar onderzoek- en onderwijsactiviteiten en steeds vaker in de reguliere bedrijfsvoering.

6.2 Uitdaging

Na de inwerkingtreding van de AVG in 2018 heeft de toezichthouder het aanzienlijk drukker gekregen. Daarbij zijn in de jaren 2017 en 2018 30 medewerkers vertrokken en zijn er circa 115 nieuwe medewerkers gestart. Dit zorgt voor veel onrust binnen de organisatie en een achterstand in het werk waarvoor ze staan.[3] In september meldt de AP dat ze het sterk toegenomen aantal klachten niet aankan.[4] Een voorbeeld van een zichtbaar gevolg hiervan is dat de Consumentenbond de AP in november 2019 formeel in gebreke stelt voor de afhandeling van het handhavingsverzoek dat ze deed

[1] https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2019Z11700&did=2019D24101
[2] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/focus_ap_202-2023_groot.pdf
[3] https://www.groene.nl/artikel/de-tragedie-van-het-privacytoezicht
[4] https://autoriteitpersoonsgegevens.nl/nl/nieuws/sterke-toename-van-privacyklachten

in het kader van een grootschalige privacy-schending door Google.[5] Dit personeelstekort en het relatief grote aantal recent gestarte medewerkers is ook voor de HvA merkbaar. De FG heeft op een aantal momenten inconsistente uitspraken met betrekking tot risico inschattingen bij een datalek gemerkt. Een ander voorbeeld is de kwaliteit van de *normuitleg grondslag 'gerechtvaardigd belang'*[6], waarop binnen de privacy-wereld het nodige commentaar is gegeven.[7]

6.3 Helder standpunt

Een aantal ontwikkelingen zorgt er wel voor dat organisaties meer richting krijgen bij de naleving van de Verordening en dat de effecten beter merkbaar worden in de reguliere bedrijfsvoering. Brancheverenigingen Nederland ICT heeft als eerste organisatie in Nederland een gedragscode opgesteld, zoals is bedoeld in art. 40 van de AVG. Deze code is verschenen en ter goedkeuring aangeboden aan de AP. De AP heeft haar ontwerpbesluit om deze code goed te keuren gepubliceerd in de Staatscourant van 12 augustus 2019.[8] Deze code kan onder meer van toepassing worden op de overeenkomsten die de HvA afsluit met leveranciers, die optreden als verwerker in opdracht van de HvA.

Verder heeft de AP op 27 november haar definitieve lijst van verwerkingen gepubliceerd waarbij zij een hoog risico ziet voor de betrokkenen en waarvoor een Data Protection Impact Assessment (DPIA) verplicht is. [9] Hiermee geeft ze helderder invulling aan de 9 breed uitlegbare punten die op 4 oktober 2017 met betrekking tot dit onderwerp in de richtsnoeren van de EDPB zijn gepubliceerd.[10] De lijst is onderdeel gemaakt van de Informatie Beveiliging en Privacy (IB&P) assessments die bij de HvA worden uitgevoerd bij nieuwe en voorgenomen verwerkingen, om te beoordelen of een DPIA nodig is. Bij de HvA is het afgelopen jaar een toenemend aantal DPIA's uitgevoerd (zie paragraaf 9.4.3).

Naast de AP hebben ook diverse toezichthouders van andere EU lidstaten zich uitgesproken over de toepassing van de AVG op diverse vlakken en onderwerpen.[11]

6.4 Boetes en schadevergoedingen

In haar *jaarrapportage meldplicht datalekken* over 2018 schrijft de toezichthouder dat ze heeft gemerkt dat niet alle meldplichtige datalekken worden gemeld.[12] Ze geeft aan dat ze zich in 2019 meer zou gaan richten op de niet gemelde datalekken en dat de onderzoeken die hieruit voortvloeien mogelijk leiden tot sancties. De FG van de HvA heeft op diverse manieren en contactmomenten de verhoogde aandacht van de AP voor dit onderwerp gemerkt.

---

[5] https://www.consumentenbond.nl/nieuws/2019/ierse-toezichthouder-moet-vaart-maken-in-google-zaak

[6] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_gerechtvaardigd_belang.pdf

[7] https://zwenneblog.weblog.leidenuniv.nl/files/2020/02/GJZ_RvE_Fd_24_dec.2019_Opinie_gerechtvaardigd_belang.pdf

[8] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ontwerpbesluit_data_pro_code_nederland_ict.pdf

[9] https://zoek.officielebekendmakingen.nl/stcrt-2019-64418.html

[10] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[11] https://privacyone.ro/2019/12/18/guidance-from-data-protection-authorities-in-2019/

[12] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/jaarrapportage_meldplicht_datalekken_2018.pdf, p. 2

Op 14 maart 2019 heeft de AP als eerste in Europa haar boetebeleidsregels aangepast om deze in lijn te brengen met de AVG.[13] Overtredingen betreffende de AVG en andere wetten waarop zij toezicht houdt zijn onderverdeeld in vier boetecategorieën. Elke boetecategorie kent en boetebandbreedte van een minimum- en een maximumbedrag. Hiermee heeft de Autoriteit zich voorbereid op strengere handhaving van de regels en op de eerste boetes onder de AVG.

Op 16 juli publiceert de AP haar boetebesluit met betrekking tot een overtreding door het HagaZiekenhuis. Dit is de eerste boete onder de AVG en deze is uitgedeeld voor een schending van de artikel 32 verplichting, om voldoende passende maatregelen te treffen om persoonsgegevens te beschermen.[14] De organisatie krijgt een bestuurlijke boete opgelegd van € 460.000, met daarbij een last onder dwangsom tot een maximum van € 300.000 voor de onvoldoende beveiliging van interne patiëntendossiers. Buiten de financiële schade is hierdoor de reputatie van het ziekenhuis op een negatieve manier geraakt. De boete en de aanleiding zijn breed uitgemeten geweest in de media.

In controle zijn

In haar boetebesluit onderbouwt de AP waarom ze het HagaZiekenhuis deze sanctie heeft opgelegd. De organisatie had geen effectieve 2-factor authenticatie voor de toegang tot bijzondere categorieën van persoonsgegevens ingericht. Hiernaast ontbrak een regelmatige controle op de logbestanden met betrekking tot toegang tot dossiers en waren er twijfels over de effectiviteit van het autorisatiebeleid van de organisatie. De organisatie had geen grip op wie toegang had tot welke gegevens en was daarmee niet in controle. De HvA verwerkt andere typen persoonsgegevens dan het HagaZiekenhuis. Met het ontbreken van geldend autorisatiebeleid en 2-factor authenticatie voor onder andere de kernsystemen is de HvA onvoldoende in controle.

Niet alleen in Nederland worden de eerste boetes onder de AVG uitgedeeld. Ook de toezichthouders in onder andere Polen, Engeland, Italië en Griekenland hebben hun eerste boetes uitgedeeld.[15] [16] [17] [18] Naar verwachting zullen Europese toezichthouders elkaar verder inspireren tot het opleggen van sancties.

Toezichthouders op andere terreinen hebben soortgelijke bevoegdheden als de AP heeft op het vlak van de bescherming van persoonsgegevens. Een voorbeeld van deze bevoegdheden werd gegeven tijdens een opvallende zaak waarbij de Autoriteit Consument & Markt een boete van 1,84 miljoen

[13] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-14586_0.pdf
[14] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_haga_-_ter_openbaarmaking.pdf
[15] https://edpb.europa.eu/news/national-news/2019/first-fine-imposed-president-personal-data-protection-office_en
[16] https://ico.org.uk/media/action-weve-taken/mpns/2614757/bounty-mpn-20190412.pdf
[17] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9101974
[18] https://www.huntonprivacyblog.com/2019/04/24/greek-dpa-issues-eur-30000-fine-for-data-protection-violation/

oplegde omdat een medewerker een WhatsApp chat verwijderde tijdens een inval.[19] Secuur omgaan met persoonsgegevens en openheid ten opzichte van de toezichthouder is belangrijk.

Naast de sancties die de AP kan opleggen voor schendingen van de AVG door organisaties, zijn ook de eerste schadevergoedingen onder artikel 82, AVG toegekend. In mei is geoordeeld dat de gemeente Deventer voor een onterechte verstrekking van persoonsgegevens van een burger een schadevergoeding van € 500,00 moet betalen.[20] In september 2019 is bepaald dat het UWV € 250,00 schadevergoeding moet betalen omdat ze gezondheidsgegevens had doorgegeven aan de nieuwe werkgever van de betrokkene.[21] Deze voorbeelden zijn relatief breed in het nieuws geweest.

7. Bijlage: Media

In de media is veel geschreven over de AVG, de bescherming van persoonsgegevens en de uitdagingen die partijen hierbij hebben. Het lijkt erop dat organisaties iets meer gewend zijn aan het bestaan van de verordening en de bijbehorende uitvoeringswet en de grootste paniek met betrekking tot de implementatie is weg. Wat nu blijkt is dat niet alleen organisaties, maar ook betrokkenen zich bewuster worden van het risico dat ze lopen wanneer hun persoonsgegevens onvoldoende worden beschermd. In de media is over het afgelopen jaar heen een aantal trends te ontdekken.

7.1 Techbedrijven

Naast de privacy schending die door de Consumentenbond is aangekaart bij de AP (zie paragraaf 6.2) zijn bekende tech-giganten in het afgelopen jaar veel in het nieuws geweest. De wetenschapper Shoshana Zuboff publiceert in januari 2019 *The Age of Surveillance Capitalism*, waarin ze beschrijft hoe technologie bedrijven omgaan met de persoonsgegevens van hun klanten. De belangen die ze hierbij hebben en de machtsdisbalans tussen bedrijf en betrokkene worden zo helder beschreven, dat ze is uitgenodigd om op 27 oktober 2019 bij VPRO Tegenlicht haar onderzoek toe te lichten.[22] Het bewustzijn met betrekking tot de manier waarop organisaties omgaan met de persoonsgegevens van hun klanten en gebruikers groeit en de ernst wordt steeds beter ingezien. *Op* 21 november publiceert Amnesty International haar document "*Surveillance Giants: How The Business Model of Google and Facebook Threatens Human Rights"*, waarin ze het stelselmatig volgen van betrokkenen en profileren door grote commerciële partijen een "*unprecedented danger to human rights*" noemt.[23] Robbert Dijkgraaf, directeur van het Institute for Advanced Study in Princeton, trekt qua subtiliteit van het probleem de vergelijking met de klimaatcrisis en spreekt zijn zorg uit voor de volgende generaties.[24]

De intensivering van de maatschappelijke discussie met betrekking tot het verlies van controle over persoonlijke gegevens, maakt dat de HvA extra aandacht moet hebben voor de manier waarop ze persoonsgegevens verwerkt. Naast de verantwoordelijkheid die ze heeft met betrekking tot haar eigen

[19] https://www.acm.nl/nl/publicaties/1-84-miljoen-euro-boete-voor-verwijderen-whatsapp-chats-tijdens-inval-acm
[20] https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBOVE:2019:1827
[21] https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2019:6490
[22] https://www.vpro.nl/programmas/tegenlicht/kijk/afleveringen/2019-2020/de-grote-dataroof.html
[23] https://www.amnesty.org/en/latest/news/2019/11/google-facebook-surveillance-privacy/
[24] https://nos.nl/nieuwsuur/artikel/2322076-te-naief-over-privacy-onze-kinderen-gaan-ons-dit-later-verwijten.html

verwerkingen, draagt ook de bewuste keuze voor specifieke technologieën en leveranciers bij aan een verantwoorde en zorgvuldige verwerking van persoonsgegevens.

7.2 Datalekken

Organisaties worden zich steeds bewuster van hun plichten met betrekking tot de afhandeling van datalekken. Dit lijkt te resulteren in een aanzienlijke toename in het aantal datalekken dat bij de toezichthouder wordt gemeld. Per maand krijgt de toezichthouder in 2019 ongeveer 2200 datalekmeldingen binnen.[25] Bij de Hogeschool van Amsterdam is deze toename niet merkbaar (zie onderdeel 10, *Bijlage*: Incidenten*)*.

Diverse media hebben geschreven over een aantal prominente datalekken zowel binnen Nederland als in andere lidstaten.

Een van de meest opmerkelijke datalekken in Nederland waarover werd gepubliceerd in 2019 is het lek bij Jeugdzorg.[26] Het lek is om twee redenen opvallend. Allereerst is het schrijnend vanwege de omstandigheden, waarbij zeer gevoelige gegevens van een kwetsbare groep mensen (én minderjarig én bijzondere privé omstandigheden) zijn gelekt. De gevolgen van een dergelijk lek kunnen de betrokkenen mogelijk nog jaren achtervolgen. Vervolgens is de technische oorzaak van het lek niet een veel voorkomende manier waarop persoonsgegevens lekken. De dossiers van circa 3000 kinderen met vervelende persoonlijke omstandigheden konden worden ingezien door onbevoegden. Het lek kon plaatsvinden doordat de organisatie een oud e-mail- en web-domein heeft laten verlopen. Journalisten hebben dit domein geregistreerd en ontvingen alle dossiers die nog naar mailadressen voor dit domein waren gestuurd. De oorzaak voor dit type incident is eenvoudig te missen. Een onvolledig beheerde technische administratie kan ervoor zorgen dat dit – zij het met minder gevoelige gegevens – ook de HvA raakt. Bij Jeugdzorg heeft de ernst van het lek in ieder geval geleid tot Kamervragen.[27]

In mei heeft ook de AP zelf melding gedaan van een datalek. De toezichthouder heeft een mail gestuurd met 38 journalisten, redacties en relaties in het CC:veld.[28] Hoewel het risico voor de betrokkene gering was, heeft de AP het goede voorbeeld laten zien.

In juli zijn bij een datalek bij de Bulgaarse belastingdienst financiële gegevens van Nederlanders gelekt.[29] Hoewel de Nederlandse Belastingdienst niet verantwoordelijk is voor deze persoonsgegevens, heeft ze toch samengewerkt met haar Bulgaarse evenknie om de betrokkenen te informeren.

Dichter bij huis is een datalek bij de UvA de oorzaak geweest dat potentieel de resultaten in het Studenten Informatie Systeem van alle studenten in te zien zijn geweest.[30] Het lek is ontdekt door studenten van de opleiding “System and Network Engineering” aan de UvA en werd veroorzaakt door

[25] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-datalekken/cijfers-datalekken-2019
[26] https://www.ad.nl/binnenland/groot-datalek-bij-jeugdzorg-dossiers-van-3000-kinderen-betrokken~a4bd9770e/
[27] https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2019Z07595&did=2019D15551
[28] https://www.computable.nl/artikel/nieuws/crm/6670704/250449/autoriteit-persoonsgegevens-blundert-met-cc-knop.html
[29] https://www.rijksoverheid.nl/documenten/kamerstukken/2019/12/18/kamerbrief-datalek-bulgaarse-belastingdienst
[30] https://www.os3.nl/_media/sis_vulnerability_.pdf

een technische onvolkomenheid in SIS. Voor de HvA was de component waarin de onvolkomenheid zit op een eerder moment al uitgeschakeld.

Op 24 december 2019 werd bekend dat er een incident speelde bij universiteit Maastricht.[31] Vanwege een infectie met gijzelingssoftware heeft de instelling geen toegang gehad tot haar gegevens in bestanden en databases. Deze waren versleuteld. Allereerst is dit incident een potentiele dreiging voor de continuïteit van de organisatie. Zonder deze gegevens kunnen de bedrijfsprocessen niet doorgaan en kunnen studenten geen onderwijs krijgen en onderzoek doen. Daarnaast moet dit type incident om twee redenen worden aangemerkt als datalek. Allereerst kan de gijzelingssoftware ook worden ingezet om (persoons)gegevens naar buiten de organisatie te sturen en onbevoegd in te laten zien door derden. Vervolgens is de eventuele vernietiging van de gegevens bij afwezigheid van een back-up volgens de AVG ook aan te merken als een inbreuk met betrekking tot persoonsgegevens.

8. Bijlage: Ontwikkelingen inzake AVG

8.1 Jurisprudentie

Gaandeweg het jaar hebben verschillende arresten helderheid gegeven aan de open normen waaruit de AVG is opgebouwd. Van het groeiend aantal uitspraken in het kader van de AVG is een aantal relevant voor de HvA.

8.1.1 Inzageverzoek en examenvragen

Onder AVG artikel 15, lid 3 heeft een betrokkene het recht om inzage te krijgen tot de persoonsgegevens die een organisatie verwerkt. De voorzieningenrechter van de Rechtbank Den Haag heeft geoordeeld dat ook examens inclusief de opmerkingen van de examinator als persoonsgegevens moeten worden gezien. De organisatie moet hiermee rekening houden bij het behandelen van dergelijke verzoeken.[32] In de nieuwe OER is opgenomen dat – zolang de bewaartermijn niet is verlopen – ook de examenvragen worden overlegd bij een inzageverzoek. De organisatie hoeft echter geen persoonsgegevens te bewaren met als enig doel te voldoen aan het inzagerecht door betrokkenen. Gegevens die zijn verwijderd om dat de bewaartermijn is verstreken (dus, het moment dat de HvA geen doel meer heeft voor de verwerking van de gegevens) vallen niet binnen het inzagerecht.

8.1.2 Cookie Consent

In oktober is er meer duidelijkheid gekomen over de manier waarop toestemming gevraagd moet worden voor het plaatsen van cookies op websites. In de zaak tegen de Duitse zaak Planet49 heeft het Hof van Justitie van de Europese Unie (HvJ-EU) geoordeeld dat een vooraf ingevuld toestemmingsformulier niet mag gelden als toestemming onder de AVG.[33] Toestemming moet een actieve wilsuiting zijn. Bij een vooraf ingevuld formulier is hiervan geen sprake. HvA handelt conform deze gedragslijn,

8.2 Richtlijnen uit de EU

De European Network and Information Security Agency (ENISA) heeft in het licht van de AVG de richtlijn “*Pseudonymisation Techniques and Best Practices*” gepubliceerd om organisaties te helpen bij

[31] https://www.maastrichtuniversity.nl/news/cyber-attack-against-um
[32] https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2019:5110
[33] http://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&doclang=EN&cid=1447493

het toepassen van deze beveiligingstechniek voor de verwerking van persoonsgegevens.[34] Hierin wordt veel van de onduidelijkheid met betrekking tot dit onderwerp weggenomen door het algemene concept toe te lichten en concrete, technische oplossingen te bieden voor onder andere onderzoek en hoger onderwijs.

De AP heeft op haar website doorverwezen naar de consultatieronde voor de richtlijnen omtrent cameratoezicht van de EDPB. Deze richtlijnen moeten meer duidelijkheid geven over de verwerking van beeldmateriaal – en dus persoonsgegevens – met behulp van zowel traditionele als slimme camera's. De publicatie van het uiteindelijke document volgt. Gezien de ontwikkelingen binnen de HvA, zowel op de vlakken van onderwijs en onderzoek als dat van bedrijfsvoering gaan deze extra richtlijnen waardevolle richting geven aan de keuzes die de organisatie moet gaan maken.

Begin november heeft de EDPB haar concept richtlijn met betrekking tot *Data Protection by Design and by Default* ter consultatie publiek gemaakt. Dit stuk geeft meer richting aan de art. 25 AVG verplichting en kan helpen bij het drastisch terugdringen van de risico's van een verwerking, door vanuit het ontwerp al uit te gaan van minimale gegevensverwerking en standaard een veilige instelling van een applicatie of inrichting van een proces. Dit document geeft concrete handvatten aan verwerkingsverantwoordelijken tijdens het inrichten van processen of het ontwikkelen van applicaties.

8.3 Aanpalende wet- en regelgeving

Privacywetgeving bestaat uit diverse onderdelen, waarvan de AVG op dit moment de meest bekende is. In 2017 is het eerste voorstel voor de ePrivacy Verordening (ePV) gepubliceerd. Onder het Finse EU voorzitterschap zijn grote stappen gezet met betrekking tot de totstandkoming van de ePV. Deze voorzitter had de ambitie uitgesproken om voor het einde van haar termijn de definitieve tekst van deze verordening naar de triloog – een informeel overleg tussen de Europese Commissie, het Europees Parlement en de Raad van Ministers – te kunnen brengen. De grootste gevolgen van deze verordening zijn de cookiewall – en wat de aanpassingen ten opzichte van de Telecomwet zullen zijn – en toestemming voor verschillende marketingproducten.[35] Hoewel het de Finse voorzitter niet is gelukt om haar ambitie waar te maken, is de verwachting dat haar opvolger, Kroatië hetzelfde doel beoogt te bereiken. In de tussentijd heeft de EDPB een opinie geschreven over de verhouding tussen de AVG en de huidig geldende ePrivacy richtlijn.[36]

8.3.1 Selectielijst Hogescholen

Om te kunnen voldoen aan AVG artikel 5.1.e moeten organisaties persoonsgegevens verwijderen waarvoor ze niet langer een doel hebben. Om onder andere deze reden is de Selectielijst Hogescholen opgesteld. Dit is een breed gedragen lijst, opgesteld door een brancheverenigingen, waarin ook rekening wordt gehouden met andere wet- en regelgeving dan de AVG. Op 10 april is een nieuwe versie verschenen van deze lijst, waarin diverse aanpassingen zijn opgenomen en waarin ook de plichten die worden opgelegd door de AVG zijn verwerkt. Hierbij moet worden opgemerkt, dat gegevens niet altijd zomaar zonder nadelige gevolgen kunnen worden verwijderd uit een applicatie. Zie verder paragraaf 9.9.

[34] https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices
[35] https://ictrecht.nl/2019/08/14/dossier-eprivacy-verordening-epv-ontwikkelingen-huidige-stand-van-zaken/
[36] https://edpb.europa.eu/our-work-tools/our-documents/stanovisko-vyboru-cl-64/opinion-52019-interplay-between-eprivacy_en

8.3.2 Archiefwet

Op 29 november is een wetsvoorstel ingediend tot intrekking van de Archiefwet 1995 en vervanging door de Archiefwet 2021.[37] Dit is een concept en moet het wetgevingstraject nog doorlopen. Naar verwachting zal de HvA hier pas in 2021 de effecten van merken. Ook dit heeft mogelijk weer gevolgen voor de Selectielijst Hogescholen.

8.4 De VS als verwerkingslocatie

Op 9 juli zijn aan het HvJ-EU vragen gesteld over de bescherming van persoonsgegevens die worden verstrekt aan organisaties in de Verenigde Staten onder de voorwaarden in de modelovereenkomst van de EU – de Standard Contractual Clauses (SCC) – of op basis van een enige overeenkomst met het Privacy Shield als beschermingsmechanisme.[38] De aanleiding hiervoor waren de onthullingen door Edward Snowden over de beperkte mate waarin organisaties in de VS, vanwege het juridische regime, de gegevens van Europese burgers kunnen beschermen. De uitkomst van deze zaak heeft potentieel grote gevolgen voor de verstrekkingen van persoonsgegevens vanuit de EU naar de VS. Op 19 december publiceerde het HvJ-EU haar oordeel. De Standard Contractual Clauses bieden volgens het hof voldoende bescherming voor de persoonsgegevens van betrokkenen die zich in de EU bevinden bij de verwerking in de VS. Er zijn echter wel grote twijfels of Privacy-Shield een adequaat niveau van bescherming biedt.[39] Mocht het Privacy-Shield niet langer als adequaat worden gezien – en mocht dit net als de voorloper ervan, Safe-Harbor, worden ingetrokken – kan dit grote gevolgen hebben voor de overeenkomsten, die de HvA heeft met partijen in de VS.

9. Bijlage: Ontwikkelingen bij HvA

9.1 Realisatie jaarplan FG

In mei 2019 heeft de FG zijn jaarplan FG 2019/2020 aangeboden aan het College van Bestuur. Dit jaarplan loopt op verzoek van het College van Bestuur gelijk met het collegejaar. Door de twee documenten jaarlijks asynchroon op te leveren, kan de FG bij het schrijven van het jaarverslag terugkijken op de realisatie van de eerste helft van zijn jaarplan. Tegelijkertijd kan hij zijn jaarverslag gebruiken als input voor bijstelling van het jaarplan.

Met name in dit onderdeel wordt steeds verwezen naar punten uit het jaarplan en wordt per punt de stand van zaken beschreven. Afwijkingen in de realisatie ten opzichte van het plan worden hier onderbouwd. Over het algemeen geldt voor de inrichting van privacy door de HvA, dat 2019 is gebruikt om de basis op orde te krijgen. In 2020 wordt gewerkt om grip op de gegevens te krijgen.

9.2 Informatiebeveiliging

Informatiebeveiliging is essentieel voor de bescherming van persoonsgegevens. Mede naar aanleiding van diverse incidenten is in het afgelopen jaar veel voortgang geboekt in de beveiliging van systemen en het netwerk. Er is in 2019 gewerkt aan diverse technische maatregelen, waarmee de HvA grip krijgt op de systemen die worden gebruikt voor de verwerking van HvA gegevens – waaronder persoonsgegevens. Als onderdeel van de maatregelen worden bijvoorbeeld de mobiele apparaten

[37] https://www.rijksoverheid.nl/documenten/kamerstukken/2019/11/29/voorstel-van-wet-tot-intrekking-van-de-archiefwet-1995-en-vervanging-door-de-archiefwet-2021
[38] https://noyb.eu/cjeu-case/
[39] https://noyb.eu/cjeu-ag-opinion-first-statement/

versleuteld, waarmee de risico's voor de betrokkenen bij diefstal of verlies worden beperkt. Hiernaast wordt veel geïnvesteerd in de faciliteiten om het netwerk nauwlettend in de gaten te kunnen houden (zie paragraaf 9.7.4). Ook is er een inhaalslag in het verkrijgen van inzicht in de dreiging in de infrastructuur geweest door een risico-inschatting te maken voor de grootste kwetsbaarheden en zijn de grootste dreigingen weggenomen.

Toch is er nog veel te doen. Informatiebeveiliging zit niet alleen in technische maatregelen. Deze moeten zijn omlijst met beheerprocedures en moeten worden verstevigd met organisatorische maatregelen. Niet in het minst moeten de capaciteit en rollen in de informatiebeveiliging governance, in lijn met de overkoepelende governance integrale veiligheid zijn vastgelegd.

De organisatie wordt geremd bij de noodzakelijke ontwikkelingen en innovaties en het op verantwoorde manier realiseren van de ambities op het gebied van onderzoek.

Punt van zorg:
Een punt van zorg blijft de beperkte capaciteit op het vlak van informatiebeveiliging. Er is onvoldoende kennis en capaciteit om eigen systemen te beveiligen en de veiligheid doorlopend te controleren. De organisatie investeert om het basisbeheer op orde te krijgen en toch is er nog voldoende ruimte voor verbetering. De organisatie moet duidelijk bepalen welke prioriteit ze aan veiligheid geeft en deze ten opzichte van andere dossiers plaatsen. Ook aan de behoefte uit de organisatie, om te worden bijgestaan bij het verantwoord omgaan met ICT middelen en de (persoons)gegevens die hiermee worden verwerkt, kan niet voldoende worden voldaan. Als direct gevolg hiervan wordt de organisatie geremd bij de noodzakelijke ontwikkelingen en innovaties en het – op een verantwoorde manier – realiseren van de ambities op het gebied van onderzoek.

9.3 Autorisatiebeleid

Een groot deel van de bescherming van persoonsgegevens hangt samen met de toekenning van de juiste autorisaties om specifieke informatie te kunnen inzien. Voor een eenduidige inrichting van de autorisaties in de applicaties waarmee persoonsgegevens zijn in te zien is specifiek beleid nodig. In 2019 is door zowel FG als CISO een start gemaakt met opstellen van autorisatiebeleid. Dit beleid moet nog een laatste redactieslag ondergaan, voor het de juiste routering kan doorlopen. Pas zodra dit beleid is aangenomen, kunnen de proces-eigenaren verantwoordelijk gehouden worden voor de risico's die voortvloeien uit een onvoldoende bescherming van gegevens door onjuiste autorisaties. Zoals te lezen in paragraaf 7.2, was het ontbreken van een deugdelijk autorisatiebeleid – en het onvoldoende naleven hiervan – de reden voor een sanctie, zoals opgelegd door de AP.

9.4 Administratie

Om te kunnen voldoen aan de verantwoordingsplicht zoals deze wordt gesteld in AVG, artikelen 5 en 24 is het bijhouden van een administratie belangrijk. De administratie helpt om de verwerkingen onder controle te hebben en te kunnen verantwoorden hoe de organisatie met gegevens omgaat. De belangrijkste onderdelen van de administratie bij het krijgen en houden van controle op verwerkingen zijn

- Het register van verwerkingen (AVG art. 30);

- Inzicht verstrekkingen aan derden met bijbehorende verwerkersovereenkomsten (AVG art. 28 lid 3);
- Register IB&P assessments en DPIA's (AVG art. 35);
- Datalekkenregister (zie paragraaf 10.4) (AVG art. 33 lid 5).

Net als in 2018 is er in 2019 nog onvoldoende inzicht in de verwerkingen van persoonsgegevens binnen de HvA. In de resultaten van de eerder genoemde audit naar de implementatie van de AVG binnen de HvA, zie ook paragraaf 9.12, is beschreven dat de registratie van de verwerkingen zoals opgenomen in het verwerkingenregister nog van onvoldoende kwaliteit is. Vanwege de grootte van de organisatie en de beperkte tijd van de privacy contactpersonen voor het onderwerp, ontbreekt ook nog een deel van de verwerkingen in het register. 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 en de HvA niet de enige organisatie is waar dit het geval is. De centrale privacy officer a.i. 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 privacy contactpersonen verbeterd op basis van de commentaren uit deze groep.

Door een onvoldoende administratie heeft de organisatie onvoldoende overzicht en inzicht in wat ze met persoonsgegevens doet. Ze daardoor niet in control.

Een onvoldoende administratie heeft drie voor de hand liggende gevolgen voor de HvA. Allereerst geeft het de organisatie onvoldoende overzicht in welke gegevens ze verwerkt, wie ze betreffen, waarvoor ze worden verwerkt en hoe ze worden beschermd. De centrale privacy officer a.i. en de privacy contactpersonen hebben deze administratie nodig als dashboard om vragen uit de organisatie te kunnen beantwoorden of incidenten met betrekking tot persoonsgegevens te kunnen onderzoeken. Vervolgens is de organisatie onvoldoende in staat om te voldoen aan de verantwoordingsplicht, waaraan elke organisatie die onder de AVG werkt zich moet houden. Dit kan zichtbaar worden bij het beantwoorden van vragen van betrokkenen – bijvoorbeeld inzageverzoeken – of de toezichthouder – bijvoorbeeld in geval van een onderzoek. Tot slot heeft de FG een goede en kloppende administratie nodig als instrument om proactief toezicht te houden. Dit belangrijke onderdeel van de kwartaalrapportages die de FG volgens jaarplan gaat opleveren, is nog onvoldoende beschikbaar. De kwartaalrapportages zijn daarom vooralsnog uitgebleven.

De privacy officer houdt de voortgang van het register bij door elke 3 maanden een privacy monitor op te stellen en te bespreken met de FG. Hierin staat te lezen wat de kwalitatieve en kwantitatieve staat van het verwerkingenregister is.

Bij het bijhouden van een administratie is de kwantiteit minder belangrijk dan de kwaliteit. Toch geven onderstaande aantallen een indicatie van hoe compleet het overzicht is. Hieronder een beknopt overzicht van de belangrijkste kerngetallen. Hierin is te zien dat er ten opzichte van de stand van zaken in 2018 voortgang is geweest.

Grip op gegevens:		
Status administratie december	*2018*	*2019*
Verwerkingen:	197	283
Verwerkers / Verwerkersovereenkomsten	x / 24	137 / 80
IB&P assessment / DPIA		20 / 18

9.4.1 Verwerkingenregister

Eén van de bevindingen tijdens de audit met betrekking tot de implementatie van de AVG in 2018, is dat het verwerkingenregister onvoldoende is gevuld – zie ook paragraaf 9.12. Hoewel er in 2019 veel is gedaan om de privacy contactpersonen te faciliteren om het register te vullen, is nog een groot deel van de verwerkingen niet opgenomen. Daarbij worden mutaties, door veranderingen in bestaande en verdwenen of nieuwe verwerkingen wisselend bijgehouden, zijn er hierbij grote verschillen tussen de organisatie-eenheden en blijft het register nog te veel een momentopname.

Uit een korte inhoudelijke analyse van het verwerkingenregister blijkt dat de beschrijving van een deel van de verwerkingen van onvoldoende kwaliteit is. Concrete voorbeelden zijn het ontbreken van bewaartermijnen en in veel gevallen een incorrecte keuze voor een wettelijke grondslag. In geen van de gevallen waar is gekozen voor AVG art. 6.1.f als wettelijke verwerkingsgrond is de wederzijdse belangenafweging gemaakt en gedocumenteerd die hoort bij de grondslag gerechtvaardigd belang.

Het niet op orde zijn van specifiek het verwerkingenregister heeft twee gevolgen.

1. De organisatie heeft onvoldoende inzicht in de verwerkingen die ze doet, weet hierdoor niet welke risico's ze loopt en kan niet de juiste maatregelen treffen om de risico's te beperken of wegnemen.
2. Het register is een van de gereedschappen waarmee de FG proactief zijn toezichthoudende taak kan uitoefenen. Dit gereedschap is alleen bruikbaar als het van voldoende kwaliteit is. Dit is nog niet het geval.

Onderzoek
De verwerkingen die worden gedaan in het kader van onderzoek ontbreken nog helemaal in de administratie. Hoewel hiervoor een goede reden is – het overzicht ontbreekt en de infrastructuur was niet geschikt om de verwerkingen te registreren – levert dit gebrek aan inzicht een hoog risico op voor de organisatie. Hierbij worden veel gevoelige gegevens verwerkt bij onderzoeken en heeft de organisatie onvoldoende zekerheid over de veiligheid ervan.

9.4.2 Verwerkers / verwerkersovereenkomsten / gegevensuitwisselingsovereenkomsten

Voor elke verstrekking van persoonsgegevens aan een verwerker moet een verwerkersovereenkomst zijn afgesloten. In het register zijn 137 verwerkers opgenomen. Volgens de huidige administratie ontbreken er nog 57 overeenkomsten. De overeenkomsten die wel zijn ondertekend en geadministreerd zijn vaak van onvoldoende kwaliteit. Vooral de beveiligingsmaatregelen zijn onvoldoende: veelal worden die ingevuld door de leverancier. De HvA heeft vanwege het al eerder aangegeven probleem bij

informatiebeveiliging geen effectieve norm voor toetsing aan beveiligingseisen en onvoldoende toetsing vindt plaats

Voor een aantal verwerkingen is een gegevensuitwisselingsovereenkomst nodig. In dit geval hebben beide partijen hun eigen doeleinden voor de verwerking en zijn ze daarvoor zelfstandig verantwoordelijk. Dit soort verstrekkingen zijn beperkt of niet in beeld. Toch komen ze voor. Daar waar ze voorkomen is veelal geen of geen juiste overeenkomst getekend.

9.4.3 DPIA's

Zodra een verwerking waarschijnlijk een hoog risico veroorzaakt voor de rechten en de vrijheden van de betrokkenen moet volgens AVG artikel 35 voorafgaand aan de verwerking een Data Protection Impact Assessment (DPIA) worden uitgevoerd.[40] Vervolgens moet de FG worden betrokken en geeft hij een advies met betrekking tot de uitgevoerde DPIA. Binnen de HvA vindt een groot aantal verwerkingen met een hoog-risico plaats en gedurende het jaar is het aantal DPIA's dat is uitgevoerd toegenomen ten opzichte van 2018. In 2019 zijn 22 DPIA's en 22 IB&P's uitgevoerd. Hierdoor is de organisatie zich beter bewust geworden van de risico's die horen bij specifieke verwerkingen. De FG is ondanks zijn formele rol bij slechts een beperkt deel van de DPIA's betrokken geweest.

Er zijn twee redenen waarom het aantal uitgevoerde assessments lager is dan het zou moeten zijn. Allereerst is er geen centraal overzicht van DPIA's en IB&P's en baseert de FG zich op gegevens uit onvolledige eigen waarneming en een decentrale uitvraag. De uitkomsten van DPIA's en IB&P's (de Informatiebeveiliging en Privacy workshop) zijn versnipperd opgeslagen, waardoor de kans bestaat dat de assessments dubbel worden gedaan, of dat er geen DPIA wordt uitgevoerd voor een verwerking met een hoog risico. Additioneel gevolg hiervan is dat de FG geen mogelijkheid om de in de assessments beschreven maatregelen te controleren en kan de organisatie daar waar nodig de assessment niet periodiek herhalen.[41] Ten tweede is het DPIA-proces tot op heden nog niet optimaal ingericht. Er is veel onduidelijkheid over de manier waarop een DPIA moet worden uitgevoerd, wie deze moet initiëren en faciliteren, welke personen moeten worden betrokken en wat de juiste routering is. Ook de vorm waarin de DPIA wordt uitgevoerd is aan verbetering toe. Na een klein anderhalf jaar te hebben gewerkt met de huidige inrichting is het tijd om te inventariseren welke lessen uit de ervaringen kunnen worden geleerd. Het feit dat de FG een verplichte rol heeft bij een DPIA moet in dit proces worden verwerkt.

9.5 Implementatie AVG

Het AVG implementatieproject is in 2018 gestart met het opbouwen van de infrastructuur die voor de organisatie nodig is om verantwoord met persoonsgegevens te kunnen omgaan. Er is een start gemaakt met het verwerkingenregister, de eerste verwerkersovereenkomsten zijn opgesteld en geadministreerd en er is veel gedaan om het niveau van bewustzijn te verhogen. In maart 2019 heeft het CvB decharge verleend aan het project en is de restpuntenlijst overgedragen aan de kwartiermaker privacy. Deze kwartiermaker heeft als taak om een governance neer te zetten, waardoor de organisatie op een gestructureerde manier de bescherming van en zorgvuldige omgang met persoonsgegevens kan garanderen. Omdat privacy niet op zich staat en verbonden is met alle andere vlakken van veiligheid, is allereerst gewerkt aan een overkoepelende governance waarin privacy, informatie

[40] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#in-welke-gevallen-moet-ik-een-dpia-uitvoeren-5879
https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-europese-privacytoezichthouders-6668
[41] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia

beveiliging en fysieke veiligheid in lijn zijn gebracht. Als specifieke inrichting van de privacy kolom is een structuur voorzien waarbij elke faculteit en dienst een privacy officer heeft. Zodra wordt gewerkt volgens deze structuur zal ook de hoeveelheid tijd en aandacht voor het onderwerp moeten toenemen.

Als onderdeel van de voorgenomen governance is de rol van de Centrale Privacy Officer a.i. ingevuld door de kwartiermaker privacy, met als doel om de capaciteitsbeperking te kunnen minimaliseren en zo de FG uit de rol van privacy adviseur te halen. Deze heeft de decentrale delen waar nodig ondersteund, gefaciliteerd en samengebracht. Hij heeft op centraal niveau de afdelingen waar verwerkingen plaatsvinden bijgestaan en gezorgd voor een verhoogd bewustzijn. Vanwege zijn dubbele rol binnen de HvA en zijn deeltijd aanstelling (over de tijd heen heeft de CPO tussen de 0.4 en de 0.6 fte gehad om zijn rol in te vullen) heeft hij alleen het hoogst nodige kunnen uitvoeren. De minder urgente zaken zijn vertraagd of worden gepland voor het moment dat de rol structureel wordt ingevuld. De privacy officer heeft in zijn werk een bewuste keuze gemaakt. Buiten de hoogst noodzakelijke adviezen aan de organisatie, heeft hij zich met name ingezet om de basis op orde te brengen en voor te bereiden op een structurele aanpak.

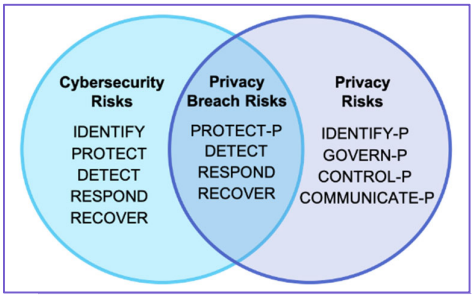
Het effect van de hier bovengenoemde aanpak is merkbaar in diverse faculteiten. Er zijn bij drie faculteiten privacy-officers benoemd. Aanvullend is in december 2019 de vacature voor de centrale privacy officer a.i. publiek gemaakt en in mei 2020 start de persoon die is geselecteerd.

9.6 Privacy en security governance

In 2019 is verder gewerkt aan de privacy en security governance binnen de HvA. In dit kader zijn veel gesprekken geweest om de geesten rijp te maken voor de in 2018 ontwikkelde houtskool schets. In 2019 hebben de kwartiermaker privacy en de kwartiermaker informatiebeveiliging gezamenlijk de directeuren bedrijfsvoering en de dienstdirecteuren gesproken over het gecombineerde belang van de twee onderwerpen en de investering die per decentraal onderdeel nodig is om ze te borgen.

Het governance voorstel gaat ervan uit dat op meerdere niveaus binnen de organisatie wordt gewerkt aan de inrichting en het beheer van de twee onderwerpen. Op centraal niveau wordt een overkoepelende structuur voorzien, waarin drie hoofd onderwerpen samen de integrale veiligheid afdekken, tw. fysieke, sociale en digitale veiligheid – met als doorsnijdende thema's: informatiebeveiliging en privacy. De functionarissen op centraal niveau hebben een functionele band met de functionarissen die op decentraal niveau met de onderwerpen bezig zijn.

Omdat het overgrote deel van de verwerkingen van persoonsgegevens in geautomatiseerde werken plaatsvindt, ligt de veiligheid van deze systemen ten grondslag aan de goede bescherming van persoonsgegevens. De verbinding tussen de privacy governance en de informatiebeveiliging governance is dus essentieel.



Figuur 1 Bron: NIST privacy framework

Aan het begin van het Project Implementatie AVG binnen de HvA in 2018, hebben de informatiemanagers van de organisatie de additionele rol privacy contactpersoon gekregen. Met de formele afronding van het project kan een aantal PCP's de uren die ze besteden aan privacy niet meer verantwoorden, zodat ze vanwege hun drukke agenda hiervoor alleen het puur noodzakelijke kunnen doen. Zaken die belangrijk,

maar minder urgent zijn krijgen niet de aandacht die ze verdienen, met als voorbeeld het bijhouden van de administratie met betrekking tot de bescherming van persoonsgegevens en de proactieve activiteiten die horen bij de bevordering van privacy-bewustzijn. Zie hiervoor verder paragraaf 12.1. Hiernaast moeten de functionarissen die bezig zijn met de bescherming van (persoons)gegevens, of dat datastewards of privacy officers zijn, in stelling worden gebracht. Dit houdt in, dat ze vroeg bij een (voorgenomen) verwerking moeten worden betrokken en dat hun inbreng zwaar moet wegen. Afwijkingen van een advies door de privacy officer of datasteward kan alleen met een goede onderbouwing. Deze stevige positie is alleen mogelijk zodra de rol is geformaliseerd.

Een punt van zorg is het tempo waarmee het besluit met betrekking tot de governance wordt genomen. De deelnemers aan het BVO hebben zich om 2019 gecommitteerd aan de governance plannen voor informatiebeveiliging en privacy. Op 29 mei 2019 is het eerste voorstel voor de privacy governance opgeleverd door de kwartiermaker. Dit is in 2019 niet vastgesteld.

9.7 Organisatie brede verwerkingen

9.7.1 Algemeen

De grootte van een verwerking van persoonsgegevens is één van de factoren die het risico voor de betrokkenen bepalen. Verwerkingen waarbij mogelijk de persoonsgegevens van alle betrokkenen van de HvA worden geraakt verdienen extra zorg en conform zijn jaarplan heeft dit de bijzondere aandacht van de FG. Voor in ieder geval drie voorgenomen verwerkingen is dit het geval geweest.

9.7.2 MS Office 365

In november 2018 heeft het Strategisch Leveranciers Management Microsoft Rijk van het Ministerie van Justitie en Veiligheid een DPIA verslag over het gebruik van Microsoft Office 365 ProPlus gepubliceerd.[42] Hierin werd duidelijk gemaakt dat met de voorgenomen implementatie van Office 365 een verwerking van persoonsgegevens zou worden geïntroduceerd die een hoog risico betekent voor alle medewerkers en studenten van de HvA. Dit was aanleiding voor de HvA om samen met de UvA een aantal eigen onderzoeken te laten uitvoeren naar zowel Office 365 ProPlus – de op een systeem geïnstalleerde versie – als de online (web) en mobiele varianten van de software. Uit deze onderzoeken bleek dat het risico voor de betrokkenen niet zozeer wordt veroorzaakt door de inhoudelijke gegevens die in de Office 365 applicaties worden verwerkt, maar door de tot de persoon herleidbare diagnostische gegevens die Microsoft krijgt over het gebruik van de applicaties. De leverancier eigent zichzelf te ruime rechten toe, ziet zichzelf onterecht als zelfstandig verantwoordelijke in plaats van verwerker van persoonsgegevens en beschrijft niet helder genoeg voor welke doeleinden ze de gegevens mag gebruiken. Gedurende het jaar is in dit kader ook de verbinding gezocht met SURF, de Rijksoverheid en de Vereniging Nederlandse Gemeenten (VNG), die met haar Informatie Beveiliging Dienst (IBD) gemeenten ondersteunt in zaken die betrekking hebben op informatiebeveiliging en privacy.

De reuring rondom dit onderwerp is in Nederland geïnitieerd en kreeg wereldwijd de aandacht. Zo heeft ook de Europese toezichthouder voor de bescherming van persoonsgegevens een onderzoek naar de privacy implicaties met betrekking tot Office 365 ingesteld.[43] Deze aandacht voor de manier waarop Microsoft omgaat met persoonsgegevens heeft ertoe geleid dat Microsoft de aanpassingen in de

[42] https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/11/07/data-protection-impact-assessment-op-microsoft-office/DPIA+Microsoft+Office+2016+and+365+-+20191105.pdf
[43] https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigates-contractual-agreements_en

voorwaarden die het Rijk, SURF en VNG gezamenlijk hebben bedongen ook aan de rest van haar zakelijke klanten gaat aanbieden.[44] Dit moet worden gezien als een groot succes dat mogelijk is gemaakt door het bestaan van de AVG.

9.7.3 MS Intune

In het FG jaarverslag 2018 is beschreven dat diefstal van onversleutelde mobiele apparaten in dat jaar één van de grootste oorzaken van datalekken was. In 2019 was dat niet veel beter en had 40% van de meldingen over inbreuken aan de FG betrekking op de diefstal of het verlies van een mobiel apparaat. Hiervan was een kwart onversleuteld. Vanwege de werkzaamheden die over het algemeen op mobiele apparaten worden gedaan moet voor elk verloren en niet versleuteld apparaat worden uitgegaan van een datalek dat moet worden gemeld bij de AP. Gecombineerd met deze zwakke plek, zorgt een incompleet overzicht van het aantal gestolen en verloren apparaten voor een potentieel hoog risico voor de organisatie. Om dit risico terug te brengen wordt een technische maatregel ingevoerd, waarmee inzicht wordt gegeven in welke apparaten in gebruik zijn en wat de versleutelingstatus hiervan is. In geval van diefstal kan het apparaat hiermee ook op afstand worden gewist.

Het invoeren van een dergelijke maatregel heeft gevolgen voor de privacy van de medewerkers van de HvA. Een externe partij heeft in een DPIA een gedegen onderzoek gedaan naar de manier waarop binnen de applicatie wordt omgaan met persoonsgegevens. Hierbij is ook onderzocht welke partijen en welke functionarissen toegang zouden kunnen hebben tot welke gegevens en hoe de bijkomende risico's kunnen worden gemitigeerd. De FG heeft een advies gegeven op het rapport dat hierover is opgeleverd. Vanwege nieuwe voorwaarden die zijn opgenomen in de overeenkomst tussen SURF en Microsoft (zie paragraaf 9.7.2) zijn voor deze verwerkingen geen hoge risico's gevonden. Met de ingebruikname van deze maatregel maakt de HvA een grote stap in het wegnemen van de risico's door datalekken en het in controle zijn van haar technische omgeving. Wel moet worden opgemerkt dat weerstand binnen de organisatie zorgt voor vertraging in de implementatie en dat er een bepaalde mate van verzet tegen de maatregel merkbaar is.

9.7.4 Logging en Monitoring

Om de veiligheid van de gegevens te kunnen garanderen en controleren en om in controle te zijn van de gegevens – en zo ook te weten wie toegang heeft gehad tot welke gegevens op welk moment – is het essentieel om acties door gebruikers op het netwerk vast te leggen en anomalieën te onderzoeken. Omdat deze faciliteit grotendeels ontbrak, heeft de CISO in de uitvoering van zijn *Verbeterplan IB*, als onderdeel van deelproject *Versterken IB ICTS* een traject opgestart om logging en monitoring in te richten. Vanwege de gevoelige aard van de loggegevens – betrokkenen worden hiermee potentieel stelselmatig en grootschalig in de gaten gehouden – is een uitgebreide DPIA uitgevoerd. Hierdoor zijn de risico's voor de betrokkenen duidelijk geworden en kan het projectteam werken aan de maatregelen om deze te beperken.

Een punt van zorg hierbij is de capaciteit voor dit onderwerp binnen ICTS. De inrichting van de maatregel kost een beperkte hoeveelheid tijd. Het dagelijks controleren van de logbestanden en het onderzoek naar afwijkende gebeurtenissen kost structureel tijd en moet worden ingericht. Ook moet de kennis om deze taak te kunnen uitvoeren worden opgebouwd en bijgehouden. Weten wat er gebeurt in de ICT infrastructuur is een belangrijke stap bij in control komen.

[44] https://news.microsoft.com/europe/2019/11/18/introducing-more-privacy-transparency-for-our-commercial-cloud-customers/

9.7.5 Onderwijsdata-analyse

Onderwijsdata-analyse is een vakgebied waar een groot belang ligt voor zowel student als organisatie. De gegevens die worden verzameld en opgeslagen in de Digitale Leer Omgeving (DLO) binnen de HvA bieden mogelijkheden voor betere begeleiding van studenten, verbetering van het onderwijs en uiteindelijk verhoging van het studierendement. Omdat hierbij wordt gewerkt met gegevens van zowel student als docent, raakt dit gebied een grote groep betrokkenen. Daarnaast zijn de gegevens die worden verwerkt zeer persoonlijk – ze leggen immers het patroon en de gewoonten vast van een betrokkene – en zijn daardoor bijzonder gevoelig. Tot slot biedt de verwerking de mogelijkheid om in het uiterste geval, geautomatiseerd conclusies te trekken over de kwaliteit van student of docent, met bijbehorende besluiten over de toekomst van een student. Geautomatiseerde besluitvorming en profilering gaan gepaard met een verhoogd risico voor de betrokkenen en moeten, indien van toepassing, met extra zorg worden behandeld.[45]

In controle zijn

SURF heeft, samen met vertegenwoordigers van een aantal instellingen, een gesprek gehad met de Autoriteit Persoonsgegevens. In dit gesprek heeft de toezichthouder uitgesproken dat “Learning Analytics een aandachtspunt is vanuit de AP”, met als gevolg dat ze met enige waarschijnlijkheid zullen terugkomen op dit dossier. Door een visie op dit punt te kunnen overleggen toont de HvA dat ze bewuste afwegingen maakt bij de verwerking van persoonsgegevens op dit vlak.[46]

Om de rechten en vrijheden van de betrokkenen te kunnen beschermen, is het belangrijk om privacy vanaf de start van ontwikkelingen op het gebied van onderwijsdata-analyse mee te nemen. Aan het begin van 2019 is vanuit het programma Digitale Leer Omgeving gestart om een visie op te stellen met betrekking tot Learning Analytics. Dit om te kunnen verantwoorden waarom bepaalde verwerkingen, conclusies en bijbehorende activiteiten op dit vlak worden gedaan. Deze visie is samen met een diverse groep partijen – waaronder de betrokkenen waarvan de persoonsgegevens in deze faciliteit gaan worden verwerkt – tot stand gekomen en wordt in het begin van 2020 voorgelegd aan het CvB.

9.8 IoT apparaten

IoT apparaten zijn alomtegenwoordig en ook bij de HvA in gebruik. Er zijn specifieke risico’s verbonden aan dit type apparaat, waarbij in veel gevallen ook persoonsgegevens zijn betrokken. Hiernaast is het bewustzijn rondom het gebruik van dit type apparaten laag. Zo heeft buiten de HvA een aantal gemeenten bij wijze van pilot deurbelcamera’s aan een groep burgers uitgedeeld om hiermee de buurt beter te beveiligen en heeft één gemeente het apparaat als inbraak werende maatregel in haar beleid opgenomen.[47] Op 13 december zijn Kamervragen gesteld over het “twijfelachtige effect en de privacy zorgen” bij deze oplossing.[48] Ook de toezichthouder ziet in deze technologie een zeker risico en heeft het in december benoemd tot een van haar prioriteiten voor de aankomende vier jaren (zie ook paragraaf 6.1).

---

[45] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp251rev01_nl.pdf
[46] *Verslag gesprek AP SURF SCIPR 9 september 2019,* p.
[47] https://www.binnenlandsbestuur.nl/digitaal/nieuws/kamervragen-over-gemeentelijke-deurbelpilots.11749734.lynkx
[48] https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2019Z25163&did=2019D51815

Binnen de HvA zijn in het afgelopen jaar diverse initiatieven geweest waarbij IoT apparaten worden gebruikt. Hoewel het nut ervan vaak groot is, moet altijd de afweging worden gemaakt of het gebruik ervan opweegt tegen de risico's voor de organisatie en haar betrokkenen. Voor in ieder geval één project is onderzocht of IoT apparatuur gebruikt kan worden om de bezetting van werkplekken te bepalen. Omdat hierbij met een camera wordt gewerkt – die de medewerker of student potentieel continue in de gaten houdt – worden de risico's zorgvuldig onderzocht en afgewogen. Het gebruik van dergelijke apparaten zal in aankomende jaren toenemen en is een punt van aandacht voor de FG. De organisatie is bezig om – analoog aan student data analyse – een breed afgestemde strategie opstellen, met daarin de relevante uitgangspunten en voorgenomen koers met betrekking tot dergelijke technieken.

Hoewel dit onderwerp niet in het jaarplan van de FG is opgenomen, gaat de hij hier vanwege de potentiele risico's voor zowel privacy als informatiebeveiliging en de additionele aandacht van de toezichthouder meer aandacht aan besteden.

9.9 Bewaartermijnen

De bewaartermijnen van de voornaamste archiefbescheiden horend bij de belangrijkste processen van een hogeschool (waaronder persoonsgegevens) zijn vastgelegd in de Selectielijst hogescholen. Deze lijst is in juni 2019 geactualiseerd naar aanleiding van de inwerkingtreding van de AVG. Voor een aantal verwerkingen maakt de organisatie voor haar bewaartermijnen een gedocumenteerde en door het CvB goedgekeurde uitzondering op de selectielijst. De bewaartermijnen zijn dus globaal beschreven en bekend binnen de organisatie. Specifieke termijnen worden tijdens de IB&P en DPIA workshops per proces besproken met de eigenaar van de verwerking die binnen een proces plaatsvindt. Toch is voor een nog onbekend aantal processen de bewaartermijn niet vastgesteld en vastgelegd in het register. De organisatie heeft dus niet in alle gevallen een bewust besluit genomen over de termijn waarbinnen persoonsgegevens mogen worden bewaard en is op dat punt nog niet in control.

Kijkend naar de complexiteit om persoonsgegevens daadwerkelijk uit applicaties te verwijderen – zonder daarmee de werking van applicaties nadelig te beïnvloeden – gecombineerd met de grootte van de verwerkingen, is het extreem complex om de bewaartermijnen na te leven. Het gevolg hiervan is dat persoonsgegevens niet worden verwijderd en nog steeds worden verwerkt nadat de bewaartermijn volgens de selectielijst is verstreken. Een punt van zorg is, dat een dergelijk complex vraagstuk met de huidige bezetting niet proactief wordt opgepakt. Geen van de – formeel of informeel – met privacy belaste functionarissen heeft de tijd om hiervoor een project op te starten, of te zorgen dat dit gebeurt.

Omdat de beperkingen bij het bepalen en naleven van bewaartermijnen op een aantal manieren risico's met zich meebrengt, zowel voor de organisatie als voor de betrokkene, blijft dit een punt van aandacht voor de FG en zal hij met regelmaat de status blijven controleren. Het eigenaarschap en de capaciteit die nodig zijn om de risico's te beperken en beter in control te zijn worden mede vergroot met een vastgestelde privacy governance.

9.10 Betrokkenheid FG

De FG is goed gepositioneerd binnen de HvA en kan onafhankelijk zijn werk uitvoeren. Hij brengt rechtstreeks verslag uit aan de hoogste leidinggevende van de verwerkingsverantwoordelijke. Hiernaast brengt hij proactief een groot deel van zijn tijd door met het spreken van sleutelpersonen binnen de organisatie, om zo te weten waar risico's voor betrokkenen bestaan en welke maatregelen deze kunnen

beperken. Hierbij spreekt hij met functionarissen op alle lagen binnen de organisatie, van strategisch tot operationeel. Met deze aanpak heeft de FG echter toch nog een beperkt beeld van wat er allemaal gebeurt en hij wordt bij veel zaken nog niet proactief betrokken.

Betrokkenheid FG
AVG artikel 38, lid 1: " *De verwerkingsverantwoordelijke en de verwerker zorgen ervoor dat de functionaris voor gegevensbescherming naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.*"

Om te verzekeren dat de FG wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens kan de HvA richtlijnen opstellen waarin is opgenomen wanneer de organisatie de FG betrekt.[49]

Met de – zij het beperkte – beschikbaarheid van een privacy officer in 2019 heeft de FG beter zijn toezichthoudende rol, zoals is beschreven in AVG, art. 39, kunnen uitoefenen. Hij is minder betrokken geweest bij adviestrajecten dan in 2018 en spreekt vooraf met de privacy officer a.i. de kaders af, waarbinnen de verwerking moet gebeuren.

Een deel van de taak van de FG is proactief toezicht uitoefenen, op basis van verschillende middelen, zoals een kloppende administratie. Ook een "Plan-Do-Check-Act" cyclus en de uitvoer van een jaarplan, zoals opgesteld door de privacy officer, zijn gereedschappen waarmee de FG beter de status van de naleving van de AVG kan meten. De status van de administratie (zie paragraaf 9.4) en de governance (zie paragraaf 9.6, 9.11) zijn momenteel beperkend voor dit aspect van het toezicht op naleving van de AVG en het in control zijn van persoonsgegevens.

9.11 Periodiek meten

Een onderdeel van de werkzaamheden die de privacy contactpersonen moeten gaan uitvoeren is de periodieke rapportage aan de centrale privacy officer a.i.. Deze rapportage gaat worden gedaan aan de hand van het privacy normenkader zoals dit wordt ontwikkeld onder leiding van SURF. Het normenkader is erg uitgebreid en het is onmogelijk om alle punten hierin in één keer uit te voeren. De centrale privacy officer a.i. is in 2019 bezig geweest met de voorbereidingen om het de privacy contactpersonen zo makkelijk mogelijk te maken. De 10 meest urgente punten uit het kader zijn als activiteiten opgenomen in het privacy jaarplan. Vanwege de gedeelde diensten zijn deze ook afgestemd met de privacy officer van de UvA. De decentrale delen kunnen met behulp van dit plan hun activiteiten uitvoeren en elk kwartaal over de voortgang rapporteren aan de privacy officer. Het is de ambitie om voor deze activiteiten dit jaar te groeien naar volwassenheidsniveau 3.

In het jaarplan FG 2019/2020 is opgenomen dat de FG elk kwartaal een rapportage stuurt naar zijn CvB portefeuillehouder. De gegevens voor deze rapportage bestaan voor een groot deel uit de resultaten die moeten worden opgeleverd door de privacy contactpersonen. Deze kunnen dit nog niet doen, omdat de governance nog niet is vastgesteld en diverse processen verhelderd moeten worden. Zodra aan deze voorwaarde is voldaan zal periodiek en in lijn met de andere kolommen binnen het integrale veiligheid

[49] WP29 *Guidelines on Data Protection Officers (DPO)*, 2016, p. 13

domein, gerapporteerd worden. De centrale privacy officer a.i. zal hierbij een faciliterende en aanjagende rol spelen. Vooralsnog kan de FG dit punt uit zijn jaarplan onvoldoende uitvoeren.

9.12 Audit op implementatievermogen AVG

In 2018 is een audit uitgevoerd om het implementatievermogen van de compliance inrichting voor de AVG bij de HvA te onderzoeken. De bevinding hieruit was dat de HvA op een aantal vlakken onvoldoende scoort. De grootste knelpunten zijn de consistentie waarmee de verwerkingen werden vastgelegd binnen de organisatie en de beschikbare capaciteit voor taken in het kader van privacy en de bescherming van persoonsgegevens. Zoals opgenomen in het jaarplan FG 2019/2020, is in Q4 de start gemaakt aan een vervolg op de audit uit 2018. Hierbij wordt specifiek gekeken naar de knelpunten uit de eerste audit. Deze audit is een stap om te zien of in 2019 de basis op orde is gebracht en om in 2020 in control te komen.

Bij het uitvoeren van de vervolg-audit wordt het gebruikte audit-kader vergeleken met het SURF normenkader dat, verwerkt in het privacy jaarplan, is voorzien als meetlat waartegen de privacy contactpersonen hun onderdeel periodiek zullen toetsen.

9.13 Cookies

Bijna elke website gebruikt cookies om beter te kunnen functioneren en goed inzicht te bieden in de bruikbaarheid ervan en het bezoek eraan. Met het gebruik van cookies op een website worden persoonsgegevens verwerkt en in veel gevallen verstrekt aan derde partijen. Door gebruik te maken van een specifiek soort cookie – het tracking cookie – kan de HvA en de eventueel externe leverancier van het cookie de bezoeker van de website volgen. De externe leverancier van het cookie kan niet alleen zien dat de bezoeker de website van de HvA bezoekt, hij ziet ook welke andere websites iemand bezoekt als die sites ook zijn cookie gebruiken.

In 2019 is meer duidelijkheid gekomen over het gebruik van cookies en cookiewalls. Een website mag niet alleen toegankelijk zijn voor diegene die akkoord gaat met het plaatsen van cookies.[50] Hiernaast, zoals te lezen in paragraaf 8.1.2, is in eind 2019 duidelijk geworden dat een vooraf ingevuld cookie consent formulier niet kan gelden als toestemming voor het plaatsen van cookies.

De websites van de HvA gebruiken geen cookiewalls en laten bezoekers ook toe als die geen cookies willen ontvangen. Op 6 september is voor de HvA websites een nieuwe manier in gebruik genomen om toestemming te vragen en te administreren. Hiermee wordt de bezoeker tegelijkertijd geïnformeerd over de verwerking van zijn persoonsgegevens. Het formulier zal continu in ontwikkeling moeten zijn om aan te blijven sluiten op de laatste ontwikkelingen op dit vlak.

9.14 Communicatie en bewustwording

In december 2018 is de projectleider begonnen, die het awareness programma gaat leiden, als een van de deelprojecten uit het Programmaplan informatiebeveiliging. Door het jaar heen zijn activiteitgericht en doelgroep specifiek diverse bewustwording-activiteiten uitgevoerd. Hierbij is zoveel als mogelijk aangesloten bij bestaande initiatieven. Om de inspanningen van het programma meetbaar te maken, is onder een grote groep studenten en medewerkers een 0-meting uitgevoerd. Dit geeft een beeld van de mate van bewustzijn met betrekking tot informatiebeveiliging en privacy. Uit de eerste bevindingen blijkt dat medewerkers en studenten behoefte hebben aan informatie over de concepten “persoonsgegevens”

[50] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_ap_cookiewalls.pdf

en “datalekken”. Ook hebben ze handvatten nodig hoe ze gegevens veilig te kunnen verwerken, opslaan en versturen.

Dit onderwerp kent twee punten van zorg. Allereerst maakt de grootte van de organisatie het uitdagend om de medewerkers en studenten tot in de haarvaten van de organisatie bewust te maken. Hiervoor zijn aanhoudende, creatieve en diverse initiatieven voor nodig. Ten tweede is bewustwording het aspect van integrale veiligheid dat als eerste wegzakt. Het moet dus een structurele taak zijn, waarvoor blijvend capaciteit voor moet worden geoormerkt.

9.15 Onderzoek

Als een van de strategische doelen van de HvA heeft onderzoek een prominente plek in de werkverdeling en is groei van de onderzoek inzet een van de ambities.[51] Veel van deze onderzoeken betreffen gevoelige en/of bijzondere categorieën van persoonsgegevens en in diverse gevallen kwetsbare groepen, zoals minderjarigen, mensen met een beperking en verslaafden.[52] [53] Een ander vlak waarop door de HvA en andere kennisinstellingen in Amsterdam aanzienlijk wordt geïnvesteerd – zowel in geld als in tijd – is onderzoek naar Artificial Intelligence.[54] Dit onderwerp, dat zwaar afhankelijk is van algoritmen, vraagt op een andere manier speciale aandacht met betrekking tot de bescherming van persoonsgegevens.[55] Vanwege de aard van het werk, kan van onderzoekers niet worden verwacht dat zij specialisten zijn waar het gaat over privacy en het verantwoord en zorgvuldig omgaan met persoonsgegevens. De ondersteuning op dit en andere relevante vlakken ligt volgens het Landelijk Coördinatiepunt Research Data Management (LCRDM) – als onderdeel van SURF – “*in toenemende mate bij specifieke personen met een dataprofiel: de datastewards*”.[56] Tegelijkertijd is de capaciteit van de datastewards bij de HvA aan het afnemen, waardoor de zorg voor de kwaliteit en veiligheid van onderzoeksgegevens – waaronder persoonsgegevens – onvoldoende kan worden gegarandeerd. Rakend aan het onderwerp governance (zie verder paragraaf 9.6) moet ook hier een kwaliteitsslag worden geslagen. Niet alleen is binnen de faculteiten onvoldoende capaciteit beschikbaar voor deze functie, ook het kennisniveau met betrekking tot de bescherming van persoonsgegevens en de positie van de – nu al bestaande – datastewards is niet in alle gevallen voldoende stevig en geborgd om privacy binnen de huidige onderzoeken te garanderen. Met een groeiende hoeveelheid en omvang van onderzoeken wordt het belang om ook op dit vlak de kwaliteit te borgen groter.

Hoewel dit onderwerp niet in het jaarplan van de FG is opgenomen, gaat de hij hier – en in het bijzonder het gebruik van algoritmen – vanwege de potentiele risico’s en de additionele aandacht van de toezichthouder meer aandacht aan besteden.

9.16 Verbinding

Als onderdeel van het jaarplan FG 2019/2020, is de FG van de HvA onderdeel geweest van een aantal groepen en gremia, heeft hij diverse conferenties en presentaties bezocht en heeft hij daar waar mogelijk ook gepresenteerd. Het hoofddoel van deze inspanning is om zoveel als mogelijk te leren van

[51] HvA jaarverslag 2018, p. 27
[52] https://www.hva.nl/akmi/projecten/projecten.html
[53] https://www.hva.nl/urban-vitality/gedeelde-content/contentgroep/mambo/resultaten/resultaten-mambo.html
[54] https://www.hva.nl/content/nieuws/nieuwsberichten/2019/12/amsterdamse-kennisinstellingen-steken-1-miljard-in-ai.html
[55] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/focus_ap_202-2023_groot.pdf, p. 7
[56] https://www.lcrdm.nl/files/lcrdm/2019-05/LCRDM%20rapport%20datastewardship_NL_online.pdf

op de HvA lijkende organisaties en lessen die de HvA heeft geleerd te delen. Daarbij helpt het de organisatie om te bepalen hoe de geldende wetgeving moet worden geïnterpreteerd en welke ontwikkelingen relevant zijn.

Elke zes weken is er overleg tussen de FG's van de hogescholen van Amsterdam, Utrecht, Rotterdam, Leiden en Saxion hogeschool. Hiernaast is elke drie maanden een overleg met de FG's van de gemeente Amsterdam, de VU, de UvA, de ACTA en de HvA. Tussendoor heeft de FG ad-hoc collegiale overleggen met FG's en andere privacy professionals van een breed scala aan publieke en private organisaties.

10. Bijlage: Incidenten

10.1 Algemeen

Hieronder staat een overzicht van de incidenten die bij de FG zijn gemeld en die dus potentieel een inbreuk in verband met persoonsgegevens betekent.

> „**inbreuk in verband met persoonsgegevens**": een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;
> AVG Art. 4.12

De FG beoordeelt meldingen op drie aspecten. Allereerst bepaalt hij of er sprake is van een datalek in de zin van de AVG. Vervolgens bepaalt hij, cf. AVG art. 33, sub 1, of het "*waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt*" voor de betrokkenen. Dit bepaalt of er een melding bij de AP moet worden gedaan. Tot slot is het de vraag of de inbreuk, cf. AVG art. 33, sub 1, "*waarschijnlijk een hoog risico inhoudt*" voor de betrokkenen van de HvA. Zodra dit het geval is, heeft de organisatie de plicht om deze betrokkenen te informeren van het voorval.

Omdat veel persoonsgegevens worden verwerkt in een geautomatiseerd systeem, is een datalek bijna altijd tegelijkertijd een informatiebeveiliging incident en omgekeerd. Daarbij wordt erop gewezen dat het onderstaande overzicht niet kan worden gezien als aanvullend op de rapportage van de CISO. Een aantal incidenten uit de rapportage van de CISO heeft geleid tot datalekken of meldingen daarvan. Een aantal datalekken is niet terug te vinden in de informatiebeveiliging-rapportage. Er is derhalve een gedeeltelijke overlap.

10.2 Vermissingen

Bij het op orde brengen van de administratie van ICT middelen is begin 2019 gebleken dat een groot aantal apparaten – zoals laptops en telefoons – vermist is. Omdat niet meer te achterhalen is welke gegevens op de systemen hebben gestaan, is het niet mogelijk om de feiten die nodig zijn voor een datalekmelding bij de toezichthouder te achterhalen. In april 2019 heeft de FG een memo aangeboden

aan het College van Bestuur, met hierin het voorstel om apparaten die voor 2019 als vermist zijn opgegeven niet te behandelen als een potentieel datalek. Dit besluit is in april genomen.

10.3 Mandaat

Bij de afhandeling van inbreuken met betrekking tot persoonsgegevens is een duidelijke trend te herkennen. Het College van Bestuur heeft de FG het mandaat gegeven om van een specifiek type incident te bepalen dat er geen melding bij de toezichthouder wordt gedaan. Zodra een inbreuk voldoet aan de onderstaande karakteristieken neemt de FG het incident op in zijn register en informeert hij periodiek zijn portefeuillehouder binnen het CvB:

- Het betreft een gestolen apparaat;
- Op het apparaat zijn geen bijzondere categorieën van persoonsgegevens aanwezig;
- Het apparaat is volgens de standaard van ICTS beveiligd en versleuteld;
- Het apparaat is voorzien van een adequaat wachtwoord of complexe pincode;
- Direct na diefstal en de melding hiervan bij het CERT heeft de gebruiker zijn of haar logingegevens aangepast;
- De diefstal van het apparaat veroorzaakt geen risico voor de rechten en de vrijheden van de betrokkenen.

10.4 Datalekkenregister

Op 29 april heeft de AP haar “handreikingen om registratie datalekken te verbeteren” gepubliceerd.[57] Het incidenten register dat de FG bijhoudt is aangepast en voldoet aan de regels zoals in deze handreiking te lezen zijn.

10.5 Datalekken

In de periode van 1 januari 2019 tot en met 31 december 2019 zijn bij de FG **47** inbreuken met betrekking tot persoonsgegevens, waarvoor de HvA verantwoordelijke is, gemeld. In de laatste vier maanden van 2018 zijn er 17 datalekken gemeld bij de FG. Door dit aantal te extrapoleren naar een volledig jaar, is te concluderen dat in 2019 minder incidenten zijn gemeld dan in 2018. Dit is in tegenstelling tot de landelijke trend, waar het totale aantal meldingen bij de AP, ten opzichte van 2018 een stijging van 29% laat zien. Dit bevestigt het idee van FG dat er, net als afgelopen jaar, veel inbreuken niet bij hem worden gemeld. Hiervoor zijn diverse redenen te bedenken. Er is een onvolkomenheid in het proces van incidentafhandeling. Hieraan wordt gewerkt. Verder, uit de 0-meting awareness uitgevoerd in opdracht van de CISO in het laatste kwartaal van 2019, moet blijken of dit komt door een onbekendheid met de concepten persoonsgegevens en datalekken (zie ook paragraaf 9.14). Op basis van de resultaten van deze meting kunnen maatregelen worden genomen om het bewustzijn te verhogen en de nodige kennis te vergroten.

Uit gegevens die zijn opgeleverd door de CISO blijkt dat het hieronder genoemde aantal meldingen met als oorzaak **Apparaat, gegevensdrager of papier kwijtgeraakt en/of gestolen** niet volledig is. Er is een groot verschil tussen het aantal van dit soort meldingen aan de FG en het aantal vermissingen en diefstallen dat wordt gemeld bij de ICTS servicedesk. Hiernaast blijkt uit het facilitair registratiesysteem voor veiligheidszaken, dat ook niet alle gevallen van diefstal of verlies worden gemeld bij de ICTS servicedesk. Er is geen centrale registratie van vermissingen en diefstallen, waardoor de organisatie

57 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handreiking_verbeteren_registratie_datalekken.pdf

niet op de hoogte is van veel potentiele datalekken en daarvoor ook geen verantwoordelijkheid en gepaste maatregelen kan nemen.

Hieronder een overzicht van het aantal meldingen van daadwerkelijke datalekken bij de FG per maand:

Tabel 1 Datalekken per maand

Maand	# datalekken
Januari	8
Februari	2
Maart	4
April	2
Mei	1
Juni	7
Juli	3
Augustus	4
September	4
Oktober	5
November	4
December	3

De toezichthouder verdeelt in haar meld-stramien en jaarrapportage de datalekken onder in een aantal categorieën.[58] Hieronder het overzicht van datalekken waarvoor HvA verwerkingsverantwoordelijke is, onderverdeeld in de categorieën, zoals in gebruik bij de AP.

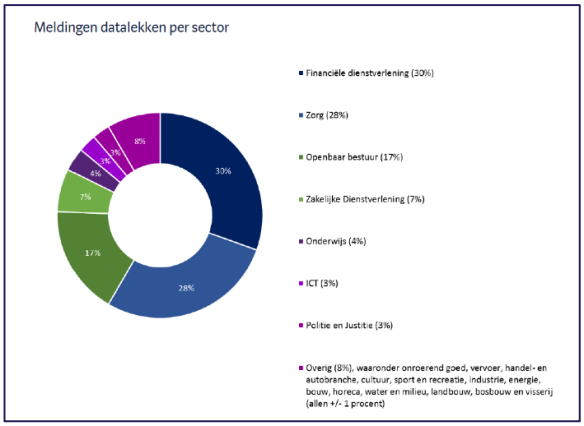
Tabel 2 Datalekken Per categorie AP

Oorzaak	Aantal
Persoonsgegevens verstuurd of afgegeven aan een verkeerde ontvanger	12
Apparaat, gegevensdrager of papier kwijtgeraakt en/of gestolen	18
Brief of postpakket kwijtgeraakt of geopend retour ontvangen	0
Hacking, Malware en/of Phishing	5
Persoonsgegevens per ongeluk gepubliceerd	12
Persoonsgegevens van een verkeerde klant getoond in klantportaal	0
Persoonsgegevens nog aanwezig op afgedankt apparaat	0
Overig	0

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

Een onderzoek binnen de SURF gemeenschap heeft de volgende gemiddelden opgeleverd, waaruit blijkt dat de HvA hoger dan gemiddeld scoort. Hiervoor is een aantal oorzaken te bedenken, zoals de mate van bewustzijn binnen een organisatie, het aantal medewerkers dat met persoonsgegevens werkt, de staat van de informatiebeveiliging en op basis van welke voorwaarden de organisatie bepaalt dat een incident een datalek is.

Soort instelling	Gem. # datalekken	Gem. # meldingen bij AP
HBO (n=15)	16,3 (HvA: 30,7 boven gem.)	4,8 (HvA: 7.2 boven gem.)
MBO (n=5)	13,6	4,2
Universiteit (n=4)	31,3	14,3



Figuur 2 Bron:Meldplicht Datalekken: Facts & Figures 2019

De onderwijssector is verantwoordelijk voor 4% van de meldingen van datalekken bij de Autoriteit Persoonsgegevens. Dit is een stijging van 1 procent ten opzichte van 2018. Het aantal lekken is gestegen van 630 meldingen in 2018 naar 1078 meldingen in 2019. In deze percentages is de omvang van de sector niet meegewogen. Binnen de vier procent wordt niet nader gespecificeerd hoeveel meldingen er zijn gedaan door primair, secundair en tertiair onderwijsinstellingen.

In controle zijn: datalekken

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.[59] Ze kondigt daarbij aan, dat ze zich hier in 2019 extra op zal richten 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.[60] 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.

59 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/jaarrapportage_meldplicht_datalekken_2018.pdf, p. 2

60 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-past-boetebeleidsregels-aan

11. Bijlage: Rechten van de betrokkenen, klachten en bezwaren

In de periode die deze rapportage beschrijft, is net als in de laatste maanden van 2018 het aantal verzoeken van betrokkenen om hun rechten uit te oefenen beperkt. In de diverse informatie uitingen met betrekking tot privacy heeft de HvA opgenomen dat inzage in en wijziging van eigen gegevens voor een groot deel mogelijk is in de daarvoor bestemde systemen.[61] [62] Hiernaast is de HvA transparant over welke persoonsgegevens voor welk doel worden gebruikt, bijvoorbeeld in de diverse toestemmingsformulieren en privacy statements. Mogelijk dat hierdoor het aantal verzoeken beperkt is gebleven.

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

In het jaar is één formele klacht ingediend met betrekking tot een verwerking. Deze is door de betreffende faculteit afgehandeld. In één geval heeft een betrokkene zich beroepen op het recht zoals beschreven in AVG, artikel 20, om bezwaar te maken tegen een verwerking. Het decentrale onderdeel van de organisatie heeft het bezwaar afgehandeld en haar procedure zo aangepast dat dit bezwaar kan worden gehonoreerd.

12. Bijlage: Risico's en adviezen

12.1 Algemeen

Er loopt een groot aantal initiatieven en projecten. De voortgang in zaken als de governance, autorisatiebeleid en diverse technische beveiligingsmaatregelen is echter onvoldoende. Uit de ontwikkelingen binnen de HvA (*Bijlage: Ontwikkelingen bij HvA*) volgt een aantal punten van zorg en een aantal risico's. Deze punten van zorg zijn hieronder gebundeld en expliciet gemaakt.

12.2 Governance

Het uitblijven van een besluit met betrekking tot de governance van integrale veiligheid zorgt voor een aantal beperkingen. Zoals beschreven in de paragrafen over Administratie (9.4) en Bewaartermijnen (9.9), is een proactieve aanpak nodig. Met de huidige werklast van de diverse medewerkers zal een

[61] https://az.hva.nl/medewerkers/staven-en-diensten/az-lemmas/medewerkers/hva-breed/juridische-zaken/avg/privacy-rechten/wat-zijn-mijn-rechten.html
[62] https://az.hva.nl/studenten/az-lemmas/studenten/hva-breed/juridische-zaken/privacy/wat-zijn-mijn-rechten/wat-zijn-mijn-rechten.html

informeel belegde taak pas worden uitgevoerd als de kerntaak van een medewerker af is. Met een vastgestelde governance kan de centrale privacy officer a.i. in geval van specifieke opdrachten een beroep doen op de tijd van de privacy contactpersonen en datastewards. Denk hierbij aan een kwaliteit slag in het verwerkingenregister, inspanningen leveren om het bewustzijn van de het decentrale onderdeel te verbeteren of het laten aanpakken van autorisaties binnen applicaties en de naleving van bewaartermijnen. Hiernaast geeft dit de medewerker de gelegenheid om zelf te herkennen op welke vlakken verbetering nodig is en kan hij zelf verantwoordelijkheid nemen voor de privacy binnen zijn faculteit of dienst.
Advies: Stel de governance vast en geef de privacy officers centraal en decentraal de positie, capaciteit en scholing die nodig is om hun taak goed uit te oefenen. Een vastgestelde governance draagt ook bij aan de verdere structurering en inrichting van zaken als het DPIA proces, de administratie en het naleven van bewaartermijnen.

12.3 Informatiebeveiliging

Vanwege de verwevenheid van informatiebeveiliging met de bescherming van persoonsgegevens levert de verbetering van de informatiebeveiliging binnen de HvA direct een verbetering op van de technische bescherming van persoonsgegevens. Zoals beschreven in paragraaf 9.2 is de veiligheid van de systemen verbeterd ten opzichte van 2018. Daarnaast is door een aantal veiligheidsincidenten het bewustzijn op dit vlak verbeterd. Toch zijn er drie zaken die nog een risico vormen voor de privacy binnen de HvA.

12.3.1 Onderzoek- en responscapaciteit

In het jaarverslag FG 2018 is gesignaleerd dat de organisatie onvoldoende onderzoek- en responscapaciteit heeft. Vanwege de beschikbare capaciteit reageert het CERT reactief en alleen op de meest urgente zaken. Belangrijke, maar minder urgente zaken worden niet afgehandeld en er wordt niet proactief gezocht naar dreigingen en (potentiele) inbreuken met betrekking tot persoonsgegevens. Hiernaast is er ruimte voor verbetering in de diverse CERT processen. Zoals te lezen in *Bijlage: Incidenten* heeft de organisatie geen compleet en correct overzicht van incidenten waarbij mogelijk persoonsgegevens zijn gelekt of vernietigd. Er is in 2019 op dit vlak geen ontwikkeling geweest, waardoor een groot risico niet is weggenomen.

12.3.2 Basisprocessen

In paragraaf 9.2 is beschreven dat de organisatie op een aantal vlakken onvoldoende is ingericht om de veiligheid van persoonsgegevens te garanderen. De adequate bescherming van gegevens begint met goed systeembeheer. De bijbehorende processen moeten de organisatie helpen om een inzicht te houden in welke systemen er in gebruik zijn, hoe goed deze beveiligd zijn en wie er wat mee kan en mag. Hoewel dit overzicht naar aanleiding van een incident in 2018 is gemaakt, is er geen proces om dit overzicht bij te houden. Uit gesprekken over diverse incidenten blijkt dat de manier waarop systemen zijn ingesteld in veel gevallen inconsistent en soms onvoldoende onderbouwd is.

Naast in controle zijn van de systemen is inzicht in de omgeving essentieel. Onverwacht netwerkverkeer kan het gevolg zijn van een digitale inbraak, waarbij persoonsgegevens geraakt kunnen zijn. Daarnaast, zodra zich een digitaal incident heeft voorgedaan moet de organisatie kunnen uitsluiten dat een persoon ongeautoriseerde toegang heeft gehad tot persoonsgegevens. De organisatie begint nu pas mondjesmaat inzicht te krijgen in wat er op technisch niveau op het netwerk gebeurt. In 2019 is hiervoor met een programma gestart. Zie ook paragraaf 9.7.4.

Advies: Richt met prioriteit het voor informatiebeveiliging relevante basisbeheer in, zoals ingezet door de CISO.[63] Zorg voor elk van deze maatregelen dat in de governance de benodigde capaciteit beschikbaar wordt gemaakt en de vereiste kennis beschikbaar is.

12.3.3 Schaduw-ICT

Vanwege de sterk decentrale inrichting van de HvA, is er slechts een zeer beperkt beeld van de technische systemen die in gebruik zijn. Op centraal niveau bestaat er een beperkt beeld van welke systemen in gebruik zijn. Het risico zit in de systemen waarvan de HvA niet op de hoogte is. Deze zogenaamde schaduw-ICT is veelal decentraal, uit eigen initiatief aangeschaft en er is vaak geen idee van hoe deze systemen beveiligd zijn. In opdracht van de CISO voert de HvA een audit uit, waaruit moet blijken welk risico de HvA hierdoor loopt.
Advies: Beoordeel de resultaten van de audit en neem de aanbevelingen over. Zorg in ieder geval voor een overzicht in de niet centraal aangeschafte applicaties en de stand van de veiligheid daarvan. Richtlijnen voor de zelfstandige decentrale aanschaf van systemen kunnen bijdragen aan de veiligheid van de gegevens die in de systemen worden verwerkt.

12.4 Administratie

Een goed kloppende en complete administratie is nodig om inzicht te hebben wat er aan gegevens wordt verwerkt. Het is het startpunt voor de privacy contactpersonen – en later de privacy officers – om maatregelen te kunnen laten nemen voor de verantwoorde verwerking. Hierbij stelt het de organisatie in staat om vragen van betrokkenen en de toezichthouder te beantwoorden.
Advies: Geef centraal en decentraal prioriteit aan het goed vullen en bijhouden van het verwerkingenregister. Zorg voor een overzicht van DPIA's, te nemen maatregelen, verstrekkingen aan derden en verwerkersovereenkomsten Dit geldt voor zowel verwerkingen in het kader van bedrijfsvoering en onderwijs als van onderzoek.

12.5 Bewustzijn

Op het gebied van de bescherming van persoonsgegevens speelt de mens een belangrijke rol en is tegelijk vaak de zwakste schakel. De HvA levert een aanzienlijke inspanning op het vlak van bewustzijn en het programma dat hiervoor verantwoordelijk is, zoals gestart onder de CISO sluit bij veel bestaande initiatieven aan. Om de haarvaten van de organisatie te bereiken met de relevante informatie en om de gecombineerde boodschap met betrekking tot informatiebeveiliging en privacy levend te houden, moet dit een doorlopende inspanning zijn.
Advies: Maak van de privacy en security bewustzijn inspanningen een permanente investering. Omdat dit programma in 2019 en 2020 is en wordt uitgevoerd als uitwerking van het verbeterplan IB van de CISO, wordt het ook gefinancierd door de CISO. Het is aan te bevelen om in 2020 de voorbereidingen te treffen om de continuïteit van de bewustzijn inspanningen te borgen.

12.6 RDM

Onderzoek en daarbij RDM heeft een prominente en groeiende plek in de organisatie. Het belang is groot en de risico's potentieel ook. Onderzoekgegevens, waaronder persoonsgegevens, moeten goed worden beschermd. Hierbij zijn twee zaken belangrijk. Allereerst moeten, zoals beschreven in paragraaf 9.15, de datastewards de juiste positie, kennis en capaciteit krijgen om als gelijkwaardige partner op te treden bij onderzoeken. Hiernaast zijn, met minimale administratieve last, overzicht in de activiteiten en

[63] https://www.cisecurity.org/controls/

onderzoeken, inzicht in risico's en maatregelen en kaders om de risico's te beperken nodig. Er loopt op dit vlak al een traject.
Advies: Zorg voor inzicht in onderzoeken en overzicht van de bijbehorende risico's. Bied vervolgens de gestructureerde aanpak en faciliteiten die nodig zijn om de data op een verantwoorde en veilige manier te kunnen verwerken, opslaan en publiceren. Geef daarnaast datastewards de tijd, scholing en positie in onderzoeken die nodig is om onderzoekers te helpen zorgvuldig met onderzoeksgegevens om te kunnen gaan. Het is belangrijk dat de adviezen van datastewards en privacy officers met betrekking tot onderzoek data zwaar wegen en er alleen met een goede onderbouwing vanaf kan worden geweken.

12.7 Richtlijn betrekken FG

Hoewel de FG in 2019 gevraagd is om bij diverse organisatie-brede ontwikkelingen aan te schuiven, is zijn betrokkenheid grotendeels beperkt geweest tot wat hij heeft opgehaald tijdens gesprekken met diverse medewerkers. Om de dossiers waarmee hij werkt niet afhankelijk te laten maken van individuele gesprekken en inzichten, is het aan te bevelen om een richtlijn op te stellen waarin is opgenomen in wat voor soort gevallen de FG moet worden betrokken. Dit is in lijn met de richtlijn van de European Data Protection Board met betrekking tot FG's.[64]
Advies: Laat de organisatie – onder leiding van de centrale privacy officer a.i. – samen met de FG een richtlijn opstellen met daarin zaken waarbij de organisatie in ieder geval de FG betrekt.

12.8 Samenvatting risico's en adviezen:

Risico	Advies
Governance	Stel de governance vast en geef de privacy officers centraal en decentraal de positie, capaciteit en scholing die nodig is om hun taak goed uit te oefenen.
Informatiebeveiliging	• Borg de kennis en capaciteit die nodig is om informatiebeveiliging naar het **gewenste niveau** te brengen; • Richt met prioriteit het voor informatiebeveiliging relevante **basisbeheer** in, zoals ingezet door de CISO; • Zorg voor een effectief CERT, om te helpen de organisatie bestand te maken tegen de groeiende digitale dreiging; • Beoordeel de resultaten van de audit naar **schaduw-ICT** binnen de HvA en neem de aanbevelingen zo veel als mogelijk over; • Voer periodiek, gezamenlijk met de UvA, een informatiebeveiliging **audit** uit bij de **gedeelde diensten**; • Voor periodiek een informatiebeveiliging **audit** uit binnen de **faculteiten**.
Administratie	Geef centraal en decentraal prioriteit aan het goed vullen en bijhouden van het verwerkingenregister. Zorg voor een overzicht van DPIA's, te nemen maatregelen, verstrekkingen aan derden en verwerkersovereenkomsten
Bewustzijn	Maak van de privacy en security bewustzijn inspanningen een permanente investering en borg deze in de organisatie.

[64] http://ec.europa.eu/newsroom/document.cfm?doc_id=44100, p. 14

Risico	Advies
RDM	Zorg voor inzicht in onderzoeken en overzicht van de bijbehorende risico's. Bied vervolgens de gestructureerde aanpak en faciliteiten die nodig zijn voor een verantwoorde en veilige verwerking. Geef datastewards de tijd, scholing en positie in onderzoeken die nodig is voor hun werk.
Richtlijn betrekken FG	Laat de organisatie – onder leiding van de centrale privacy officer – een richtlijn opstellen met daarin zaken waarbij de organisatie in ieder geval de FG betrekt.