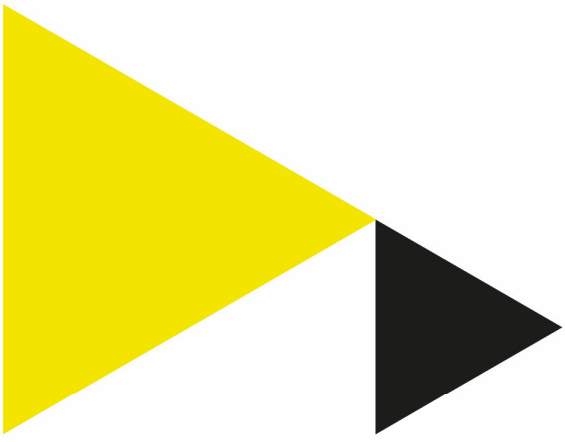
Hogeschool van Amsterdam

# Jaarverslag FG 2020

Functionaris voor Gegevensbescherming
2020 – 2021



Creating Tomorrow

# Jaarverslag FG 2020

**Author**
Martijn de Hamer

**Date**
18-May-21

**Version**
1.0

# 1. Inleiding

2020 was een jaar waarin de HvA te maken kreeg met de Covid-19 pandemie. Het coronavirus heeft grote gevolgen gehad. Thuis werken, thuis studeren en thuis onderwijs volgen was de norm. Hiermee kwam het online vergaderen, lesgeven en toetsen in een stroomversnelling en werd alleen het hoognodige fysieke onderwijs toegestaan. Dit heeft tot gevolg gehad dat de middelen die dit mogelijk maken versneld werden aangeschaft, dat bijbehorende huis- en gedragsregels moesten worden opgesteld en dat medewerkers getraind moesten worden in het gebruik.

Dit jaarverslag geeft weer in welke mate HvA in 2020 heeft voldaan aan vereisten van de Algemene Verordening Gegevensbescherming (AVG). Het is onderverdeeld in vijf delen. Allereerst reflecteert de FG op het jaarverslag informatieveiligheid van het team Integrale Veiligheid, zoals opgesteld door Chief Information Security Officer (CISO) en de Privacy Officer (PO). Vervolgens beschrijft het de activiteiten van de FG in 2020 en prominente relevante activiteiten binnen de HvA in 2020. Hierna volgt een vooruitblik op ontwikkelingen die in 2021 relevant zullen worden voor de bescherming van persoonsgegevens binnen de HvA. Tot slot beschrijft het de prioriteiten en aandachtspunten van de FG in hogeschooljaar 2021/2022.

Gezien de primaire doelgroep kan dit verslag losstaand van het jaarverslag informatieveiligheid worden gelezen. Het verslag wordt geschreven voor het College van Bestuur van de HvA. Volgens privacybeleid wordt het aangeboden aan de Centrale Medezeggenschapsraad. Het verslag wordt ook als bijlage meegeleverd met het jaarverslag informatieveiligheid, zoals opgesteld door de PO en de CISO.

# 2. Jaarverslag Informatieveiligheid

## 2.1 Jaarverslag Privacy Officer

In het Informatieveiligheid jaarverslag 2020 heeft de Privacy Officer een belangrijk deel opgenomen over de bescherming van persoonsgegevens binnen de HvA. Hierin is te lezen hoe de organisatie zich het afgelopen jaar heeft ontwikkeld op het gebied van privacy en welke stappen er zijn gezet om de bescherming van persoonsgegevens te verbeteren. Ondanks de pandemie waarmee de HvA te maken kreeg en veel van de instelling heeft gevraagd om versneld over te schakelen op volledig online werken en studeren, heeft de HvA tijd geinvesteerd om op kritieke punten een extra inspanning te leveren. Zo is zorgvuldig gekeken naar de risico's met betrekking tot diverse prominente en essentiele verwerkingen. Als voorbeeld is te noemen Proctorio, waarbij – ondanks het tempo waarin dit in gebruik genomen moest worden – oog is gehouden voor de veiligheid van het tool en de tijd is genomen om eerst een DPIA uit te voeren. Het belang van een grondige DPIA bij dergelijk risicovolle verwerkingen is in 2020 door de rechtbank Amsterdam aangetoond.[1] Ook is de HvA zorgvuldig te werk gegaan met de eerste organisatie-brede stappen met betrekking tot studentdata analyse, of wel Learning Analytics.

[1] https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2020:2917

In het jaarverslag wordt tevens ingegaan op de ontwikkelingen met betrekking tot de drie risicogebieden die in het jaarverslag van de FG 2019 zijn beschreven, Governance (paragraaf 2.2); Administratie (paragraaf 2.3); informatiebeveiliging (paragraaf 2.4). Aparte aandacht gaat uit naar de inbreuken met betrekking tot persoonsgegevens (paragraaf 2.5). De FG kan zich vinden in de bevindingen van de PO en steunt de activiteiten zoals beschreven in paragraaf 4.3 van het jaarverslag Informatieveiligheid.

## 2.2 Governance

In 2019 is de privacy-specifieke governance vastgesteld. In 2020 is de overkoepelende integrale veiligheid governance is in 2020 vastgesteld. Deze combinatie zorgt voor een solide inrichting. Binnen de contouren die worden gevormd door de governancestukken, kan in lijn met het bestuursmodel van de HvA worden doorgebouwd aan de capaciteit die nodig is om het onderwerp verder te brengen. Deze capaciteit was in 2020 nog niet op orde. Niet alle decentrale onderdelen hadden een privacy officer en in 2021 zal de beschikbare capaciteit voor het onderwerp worden geevalueerd.

In de governance Integrale Veiligheid staat een dynamisch lijst van processen en producten opgenomen. In het jaarverslag van de PO staat dat in 2020 een start is gemaakt met de geprioriteerde ontwikkeling van de voor privacy relevante producten.

## 2.3 Administratie

De AVG verplicht een organisatie verschillende soorten informatie en activiteiten met betrekking tot persoonsgegevens te registreren. De HvA heeft in 2020 veel werk verzet om deze administratie te verbeteren. Er blijft voor zowel de kwaliteit van de registratie als de volledigheid voldoende ruimte voor verbetering. Omdat het goed invullen en bijhouden van het verwerkingenregister complex blijkt is de Privacy Officer gestart met een verbeteraanpak, waarmee de privacy officers van de decentrale delen met inhoud en/of met planning worden ondersteund. Als onderdeel van deze verbeteringen wordt het bijbehorende proces integraal uitgeschreven. Verder wordt in het kader van onderzoek een data management portal ontwikkeld door RDM ondersteuning binnen de HvA. Dit portal wordt zo ingericht dat het direct ook kan dienen als register van verwerkingen voor onderzoek.

De ongeldigverklaring van het EU-VS Privacy Shield, op 16 juli 2020 was aanleiding voor extra onderhoud aan het register.[2] De Europeese toezichthouders voor de bescherming van persoonsgegevens hebben geoordeeld dat verstrekkingen van persoonsgegevens aan partijen in de VS onder dit verdrag onvoldoende waarborgen bood voor de veiligheid. Persoonsgegevens mogen alleen nogmaar aan de VS worden verstrekt onder de voorwaarden die zijn vastgelegd in de standaard EU modelovereenkomst.[3] De HvA moet hierdoor contracten met partijen in de dit land inventariseren en aanpassen naar dit model. De Privacy Officer op centraal niveau werkt aan de hand van een plan van aanpak samen met de decentrale privacy officers om verstrekkingen aan de VS weer binnen de wet te laten verlopen.

Naast de registratie van verwerkingen, is ook gewerkt aan een risico-register. Hierin worden door decentrale privacy officers en de Privacy Officer lopende en afgeronde Informatiebeveiliging en Privacy

[2] https://autoriteitpersoonsgegevens.nl/nl/nieuws/privacy-shield-voor-doorgifte-naar-vs-ongeldig-verklaard
[3] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

controles (IB&P) en Data Protection Impact Assessments (DPIA) geregistreerd.[4] Per assessment worden de risico's en bijbehorende maatregelen in dit register vastgelegd, waardoor de HvA meer grip krijgt op de risico's die ze loopt.

### 2.4 Informatiebeveiliging

In het kader van informatiebeveiliging loopt de doorontwikkeling. Het blijkt op zowel centraal als decentraal niveau een complex onderwerp, hetgeen onder andere merkbaar is in de hoeveelheid vragen die leven bij de privacy officers in de decentrale eenheden. Dit wordt bevestigd door de analyse van de afgesloten verwerkersovereenkomsten, waarin vaak onvoldoende en in voorkomende gevallen geen maatregelen zijn opgenomen.

### 2.5 Datalekken

Binnen de HvA is geconstateerd dat het aantal gemelde datalekken bij de FG in 2020 lager is dan 2019. Waar in 2019 53 meldingen zijn gedaan, heeft de FG in 2020 37 meldingen ontvangen. Deze daling – van 30% – is niet in lijn met de landelijke ontwikkeling – een daling van 11%. De oorzaak hiervan zou deels verklaard kunnen worden doordat medewerkers tien van de twaalf maanden thuis hebben gewerkt. In Q4 2020 is om deze reden een audit naar het proces van datalekken gestart. De HvA is nog in afwachting van de resultaten waaruit zal blijken wat de oorzaak is. Parallel aan de audit is in het najaar van 2020 de Privacy Officer gestart met het opstellen van een integraal proces voor het melden van datalekken.

# 3. Activiteiten FG

### 3.1 De functie van de FG

De functie van de FG staat beschreven in de AVG[5]. Vanuit deze functie informeert en adviseert hij de verwerkingsverantwoordelijke over haar verplichtingen met betrekking tot de bescherming van persoonsgegevens. Hij ziet toe op de naleving van de AVG, andere gegevensbeschermingsbepalingen (zoals bijvoorbeeld de ePrivacy richtlijn) en het privacybeleid van de organisatie en heeft hierbij aandacht voor de adequate toewijzing van verantwoordelijkheden. Desgevraagd geeft hij advies bij DPIA's. Betrokkenen kunnen over alle aangelegenheden die betrekking hebben op de verwerking van persoonsgegevens contact opnemen met de FG. Tot slot treedt de FG op als contactpersoon voor de toezichthoudende autoriteit, de Autoriteit Persoonsgegevens.

### 3.2 De FG binnen de HvA

De FG van de HvA is sinds 1 september 2018 Martijn de Hamer. Hij heeft in 2020 geen andere functies binnen de HvA gehad, en daardoor is er geen sprake geweest van mogelijke verstrengeling van belangen. Hij heeft zijn werk volledig in onafhankelijkheid kunnen uitvoeren en heeft geen beperkingen ervaren tijdens de uitvoer van zijn taak. In dit jaar heeft hij maandelijks regulier overleg gehad met de hoogste leidinggevende van de organisatie – de (waarnemend) voorzitter van het college van bestuur.

---

[4] Een IB&P is een korte beoordeling van de risico's van een verwerking, om te bepalen of de grotere tijdsinvestering van een DPIA nodig is.
[5] AVG art. 39(1)

Daar waar nodig heeft hij ad-hoc en op niet-reguliere momenten contact met deze persoon waar het urgente zaken betreft.

De FG is goed aangesloten bij de activiteiten die de PO uitvoert ter verbetering van de bescherming van persoonsgegevens bij de HvA.

Medewerkers en studenten nemen regelmatig contact op met de FG. Daar waar zij vragen hebben over de uitvoer van het beleid, verwijst hij ze naar die functionaris die het beste de vraag kan beantwoorden. In 2020 namen studenten contact op om hun zorgen te uiten over met name de inzet van online proctoring. Ook heeft de FG diverse zorgen gehoord met betrekking tot verwerkingen die nodig zijn om te kunnen thuis werken en studeren – zoals het gebruik van Office365 en Brightspace. Adequate informatievoorziening heeft de grootste zorg kunnen wegnemen.

De invloed van COVID-19 is merkbaar in de uitvoer van het werk van de FG. Hoewel hij wordt betrokken bij zaken waarbij de bescherming van persoonsgegevens van belang is, is het op afstand werken nadelig voor zijn informatiepositie. Met het wegvallen van de toevallige gesprekken met collega's is ook de serendipiteit uit zijn werk weggevallen en hoort hij minder over relevante ontwikkelingen, activiteiten en initiatieven dan hij zou moeten. Over het algemeen wordt de FG nog niet voldoende betrokken. Een mogelijke oorzaak is onbekendheid in welke situaties hij betrokken moet worden. De PO zal in 2021 hiervoor ter ondersteuning en op basis van de AVG en de handleiding AVG van de Rijksoverheid een protocol opstellen.

## 3.3 Overleggen

Naast de maandelijkse overleggen met de voorzitter van het College van Bestuur, is de FG afhankelijk van informatie over zaken die betrekking houden met de bescherming van persoonsgegevens. Een groot aantal terugkerende overleggen helpt hem inzicht te hebben in de manier waarop de HvA omgaat met persoonsgegevens en zo hoe ze zich houdt aan de geldende wet- en regelgeving en haar eigen beleid. De PO en de FG hebben aan het begin van elke week een overleg, waarin wordt terug- en vooruitgekeken. Tussendoor hebben ze veel ad-hoc overleggen om de lijn met betrekking tot voorgenomen verwerkingen, adviezen en gesignaleerde risico's te bespreken. Elke week sluit de FG aan bij het AVG overleg met Juridische Zaken en de PO, waar de puur juridische kant van dataprotectie binnen de HvA wordt besproken. Voor de afstemming rondom de met de UvA gedeelde diensten is elke week een overleg met de FG van de UvA, de Chief Information Security Officer (CISO) en de PO's van beide organisaties. Wekelijks hebben de CISO van de HvA/UvA en de FG een overleg met betrekking tot de informatiebeveiliging-specifieke ontwikkelingen. Voorts is er onder leiding van de teamleider Integrale Veiligheid een wekelijks overleg met de leden van dit team en zijn er terugkerende overleggen met de directeur bedrijfsvoering van de faculteit Maatschappij en Recht, als portefeuillehouder informatiebeveiliging en privacy binnen het BVO, en de Digital Transformation Officer, als leidinggevende van de afdeling digitale strategie & informatiebeleid (DSI).

## 3.4 Samenwerkingen en Ontwikkelingen

Ook in 2020 is de FG buiten de HvA onderdeel geweest van een aantal samenwerkingsverbanden, waarmee de HvA kan profiteren van de lessen die andere instellingen hebben geleerd en de HvA anderen kan helpen met lessen die zij zelf heeft geleerd. De FG is aangesloten bij een privacy-groep, bestaande uit FG's en PO's van zes HBO instellingen, die eens per zes weken bij elkaar komt. Samen met de gemeente Amsterdam, de VU, de UvA, ACTA en het AMC heeft de FG van de HvA elke zes weken een overleg. In Vereniging Hogescholen-verband wordt – parallel aan een dergelijk netwerk bij de

universiteiten – gewerkt aan een FG netwerk voor hogescholen. De FG van de HvA is betrokken bij de planvorming en de eerste opzet van dit netwerk.

Buiten de reguliere overleggen, is de FG gevraagd deel te nemen aan presentaties en bewustwording activiteiten voor diverse afdelingen. Zo is hij onder andere aangesloten bij sessies die zijn georganiseerd voor en door Alumnirelaties, SIS en FBE. Ook heeft hij in 2020 zijn jaarverslag 2019 toegelicht voor de leden van de Centrale Medenzeggenschaps Raad.

Buiten periodieke externe overleggen, werkt de FG van de HvA ook mee aan diverse externe initiatieven om dataprotectie in het onderwijsveld te bevorderen. Zo is hij in maart 2020 voorzitter geworden van de werkgroep Privacy in het project: Nationaal Platform Praktijkgericht Onderzoek (NPPO), is hij in februari 2020 voor het eerst betrokken bij de doorontwikkeling van een visie op studentdata analyse – onder leiding van SURF – en heeft hij deelgenomen aan de werkgroep die samen met de VH, de VSNU, SURF en KPMG een (nog uit te brengen) “Handreiking Privacy Governance” heeft opgesteld. In oktober 2020 is hij betrokken geweest bij het beantwoorden van vragen door de AP aan de VH, met betrekking tot een sectorbeeld over HBO instellingen en heeft hij in een aantal gesprekken met de AP toegelicht wat de complexiteit van de sector is en welke stappen instellingen gezamenlijk zetten om het onderwerp dataprotectie verder te brengen.

### 3.5 Contact met de AP

De FG heeft in 2020 geen contact gehad met de AP in het kader van meldingen van datalekken. Wel, zoals te lezen in paragraaf 3.4, is er contact geweest met betrekking tot het sectorbeeld hoger onderwijs.

### 3.6 Professionalisering van de FG

Om zijn deskundigheid in stand te houden (cf. AVG art. 38(2)), is de FG aangesloten bij het Nederlandse Genootschap Functionarissen Gegevensbescherming (NGFG) en de Vereniging Privacy Recht (VPR). Hiernaast is hij aangesloten bij de Informatiebeveiliging en Privacy netwerken van SURF (SCIRT en SCIPR) en heeft hij in 2020 (grotendeels digitaal) de kennisbijeenkomsten bezocht die worden georganiseerd door deze netwerken.
Om bij te blijven bij de ontwikkelingen rondom dataprotectie en relevante aanverwante juridische onderwerpen en voor zijn doorontwikkeling, is de FG in 2020 gestart met een opleiding Rechten en Digitale Technologie, waarin de juridische kant van privacy, dataprotectie, ethiek en informatiebeveiliging centraal staat.

# 4. De HvA in 2020

In maart 2020 is van de een op de andere dag de hele organisatie omgeschakeld naar digitaal thuis werken en leren. Hoewel de organisatie hierop al deels was voorbereid is toch een aantal wijzigingen met spoed doorgevoerd. Om medewerkers en studenten het nodige gereedschap te bieden om vanuit huis te kunnen werken en studeren, is onderzocht of Zoom of Slack hiervoor bruikbare middelen zouden zijn. De risico’s van het gebruik van deze applicaties waren onbekend, terwijl veel tijd is geinvesteerd in de Microsoft Office 365 applicaities, waaronder Teams, dat vergelijkbare functionaliteit biedt. DSI en ICTS hebben hierover in samenspraak met informatiebeveiliging en privacy functionarissen een weloverwogen besluit genomen.

Een aantal ontwikkelingen heeft bijgedragen aan de verbetering van de bescherming van persoonsgegevens binnen de HvA.

1. De bescherming van persoonsgegevens staat serieus op de agenda bij het bestuur van de organisatie. Er wordt tijd voor vrijgemaakt in de agenda's van de bestuurders, de risico's met betrekking tot privacy worden meegewogen bij besluiten over bestaande en nieuwe initiatieven (zoals de diversiteitmonitor van het CBS) en het is een onderwerp op de relevante agenda's van de Vereniging Hogescholen en SURF;
2. De overkoepelende governance Integrale Veiligheid is vastgesteld;
3. Als onderdeel van de governance Integrale Veiligheid zijn de activiteiten geinventariseerd die nodig zijn om de basis op orde te krijgen op het gebied van privacy;
4. In 2020 Q2 is de algemene AVG audit afgerond;
5. De werkagenda Privacy is opgesteld (a.d.h.v. punten 3 en 4), als onderdeel van de werkagenda integrale veiligheid;
6. In mei 2020 is de Privacy Officer op centraal niveau gestart (0,8FTE);
7. De groep privacy officers op decentraal niveau is aan het professionaliseren en begint, onder leiding van de PO een team te worden;
8. Het maandelijkse Privacy Officers overleg wordt steeds waardevoller, er wordt gezamenlijk gewerkt aan organisatie-brede vraagstukken en de groep wordt hechter, waardoor ze elkaar ook buiten de overleggen weten te vinden;
9. In Q3 is een start gemaakt met de audit naar het datalekken proces;
10. De PO heeft, in samenwerking met de UvA, het datalekkenproces geevalueerd en verbeterd;
11. In samenwerking met de afdeling communicatie is een start gemaakt met het verbeteren van de structuur van het Privacy lemma in de A-Z lijst;
12. Er zijn diverse awareness-sessies en presentaties bij verschillende afdelingen en faculteiten geweest;
13. Er is een terugkerend overleg ingericht tussen Integrale Veiligheid en DSI/DTO, om zo digitale ontwikkelingen en de veiligheidsbelangen van de organisatie beter te kunnen laten aansluiten;
14. Het team Integrale veiligheid is hechter gaan samenwerken en opereert beter als een multidisciplinaire eenheid. Zo zijn de werkagenda's voor de verschillende dossiers op elkaar afgestemd, wordt bij incidenten de impact van de drie aspecten van integrale veiligheid gezamenlijk beoordeeld en wordt tijdens de overleggen waardevoller informatie uitgewisseld;
15. Er is gestart met de ontwikkeling van een applicatie waarin het register van verwerkingen (cf. AVG art. 30) in het kader van onderzoek kan worden bijgehouden;
16. Er is gestart met de ontwikkeling van een applicatie, waarin het register van risico's, als onderdeel van het IB&P en DPIA proces, kan worden bijgehouden;
17. De inventarisatie van verstrekkingen aan de VS, onder het Privacy Shield, is gestart en de aanpassingen van de overeenkomsten worden geprioriteerd op basis van het risico;
18. De PO en de afdeling Juridische Zaken zijn bezig om de procedure voor verzoeken in het kader van de rechten van betrokkenen te evalueren en verbeteren.

Buiten de positieve ontwikkelingen heeft de FG een aantal aandachtspunten:

- In lijn met de bevindingen van de CISO en zoals genoteerd als bevinding in het Jaarverslag FG 2019, is informatiebeveiliging – als essentiele factor bij de bescherming van persoonsgegevens – een zorgpunt;
- Actualiteiten en de verdeling van expertise over de organisatie heen lijken een gestructureerde awareness-aanpak in de weg te staan;

- Decentrale inrichting van bepaalde processen zorgen voor een suboptimale bescherming van persoonsgegevens. Denk hierbij aan incomplete registratie van mobiele ICT middelen of toegangsrechten tot applicaties (en daarmee persoonsgegevens) die niet worden afgenomen zodra een medewerker deze niet meer zou moeten hebben;
- Zoals blijkt uit de rapportage van de PO, is het aantal datalekmeldingen in tegenstelling tot de trend die wordt gerapporteerd door de toezichthouder, gedaald. De aanname is dat (potentiele) datalekken niet worden herkend en/of niet worden gemeld;
- De capaciteit van de privacy officers van de decentrale delen is in 2020 onvoldoende geweest, zodat – op uitzonderingen na – alleen de urgente zaken worden afgehandeld;
- Het verwerkingenregister is – deels vanwege het gebrek aan capaciteit – nog onvoldoende gevuld en van onvoldoende kwaliteit;

# 5. De HvA in 2021

Vooruitkijkend naar 2021 is een aantal ontwikkelingen relevant. Gezien ontwikkelingen rondom COVID-19 is de verwachting dat studenten en medewerkers in het studiejaar 2021-2022 weer meer op locatie kunnen studeren en werken. Dit heeft gevolgen voor de noodzaak van bepaalde verwerkingen. Een belangrijk voorbeeld is online proctoring. In reactie op de risicoinschatting die hiervoor is gedaan, heeft de FG opgenomen dat de pandemie kan dienen als deel van de rechtvaardiging van de inbreuk op de privacy van de student. Ook wanneer fysiek onderwijs weer volledig mogelijk is, kan de HvA ervoor kiezen om online onderwijs te handhaven. Echter, zodra de situatie verandert – en daarmee rechtvaardiging wegvalt – moet het gebruik van deze techniek worden heroverwogen en/of opnieuw een risicoinschatting worden gedaan. De lessen die de HvA in 2020 heeft geleerd dragen bij aan een gedegen inrichting. Andere aandachtspunten zijn:

- De capaciteit van de privacy officers, decentraal, wordt in 2021, volgens afspraak geevalueerd;
- Er wordt een audit uitgevoerd naar het Data Protection Impact Assessment (DPIA) proces;
- De FG zal aandacht hebben voor de doorontwikkeling van het SURF Audit normenkader en, in lijn met de ontwikkeling in de sector, de toepassing hiervan binnen de HvA;
- De aankomende ePrivacy Regulation (met daarin de regels met betrekking tot het gebruik van Cookies op websites) wordt mogelijk van kracht – mogelijk met gevolgen voor websites van de HvA;

# 6. Activiteiten FG 2021

Een deel van de de activiteiten die door de FG worden uitgevoerd, wordt bepaald door zijn wettelijke taak. Daarnaast heeft hij, buiten actuele en aankomende ontwikkelingen – zoals deels hierboven genoemd – drie bijzondere aandachtsgebieden. Op basis van factoren zoals prioriteiten van de AP, het risico van de verwerking voor de betrokkene en de ontwikkelingen binnen de HvA zal de FG in 2021 aandacht hebben voor de volgende onderwerpen:

- Internet of Things (IoT) apparaten, volg soft- en hardware – zoals gezichtsherkenningstechnieken –, AI en algoritmen;
- Onderwijsdata analyse;
- Bewustwording m.b.t. de bescherming van persoonsgegevens.