Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

35 925 VIII **Vaststelling van de begrotingsstaten van het Ministerie van Onderwijs, Cultuur en Wetenschap (VIII) voor het jaar 2022**

26 643 **Informatie- en communicatietechnologie (ICT)**

32 761 **Verwerking en bescherming persoonsgegevens**

Nr. 190

BRIEF VAN DE MINISTERS VAN ONDERWIJS, CULTUUR EN WETENSCHAP EN VOOR PRIMAIR EN VOORTGEZET ONDERWIJS

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 14 juli 2022

Inleiding

In deze brief gaan wij in op digitaal veilig onderwijs en onderzoek. Het is belangrijk dat elke leerling, student en wetenschapper in een veilige omgeving onderwijs kan volgen en onderzoek kan doen. Niet alleen in het fysieke gebouw, maar ook in het digitale domein dat in toenemende mate deel uitmaakt van het onderwijs en onderzoek.[1]

Digitalisering zet druk op onze publieke waarden; op principes als veiligheid en privacy.[2] Steeds meer gegevens over leerlingen en studenten worden opgeslagen en uitgewisseld. Onderwijsinstellingen en onderzoeksinstellingen zijn in toenemende mate doelwit van cyberaanvallen. Voor instellingen wordt het steeds moeilijker om de privacy van leerlingen en studenten te beschermen tegen digitale dreigingen. Gegevens over leerlingen en studenten kunnen op straat komen te liggen en de continuïteit van het onderwijs kan in gevaar komen wanneer systemen niet meer benaderbaar zijn.

De digitale weerbaarheid moet daarom bij alle instellingen worden verhoogd naar een niveau dat aantoonbaar veiligheid biedt. Dit blijkt ook uit adviezen van de Autoriteit Persoonsgegevens, het Rathenau Instituut en de Inspectie van het Onderwijs.[3]

In deze brief kunt u hier meer over lezen. Daarmee komen we alle toezeggingen na die in op 1 december 2021 aan u zijn gedaan in het debat

[1] Kamerstukken 31 293 en 31 289, nr. 611.
[2] Kamerstuk 26 643, nr. 842.
[3] Kamerstukken 32 034 en 32 761, nr. 40, https://www.rathenau.nl/nl/digitaal-samenleven/naar-hoogwaardig-digitaal-onderwijs, Kamerstukken 31 288 en 26 643, nr. 918.

kst-35925-VIII-190
ISSN 0921 - 7371
's-Gravenhage 2022

over digitalisering en privacy in het onderwijs.[4] Daarnaast reageren we op verzoek van de vaste commissie voor Onderwijs, Cultuur en Wetenschap van 16 juni 2022 op het rapport van Human Rights Watch over de privacy van leerlingen in coronatijd.[5]

Leeswijzer

In paragraaf 1 beschrijven we de gemeenschappelijke uitgangspunten die we hanteren voor de hele onderwijs en -onderzoeksector.

Omdat de risico's en de mate van volwassenheid tussen sectoren verschillen, behandelen we daarna hoe de afzonderlijke sectoren de digitale veiligheid verhogen. Paragraaf 2 behandelt de maatregelen voor primair en voortgezet onderwijs en paragraaf 3 voor hoger- en middelbaar beroepsonderwijs en de onderzoeksinstellingen.

In paragraaf 4 gaan we in op de overige toezeggingen uit het debat waaronder onze reactie op een artikel in de Mare van 17 november 2021.

1. Gemeenschappelijke uitgangspunten

Vrijblijvendheid is geen optie als het gaat om digitale weerbaarheid en privacy. Het hele onderwijs en alle betrokken partijen moeten stappen nemen om de digitale weerbaarheid in de hele sector te verhogen, en om de continuïteit en kwaliteit van het onderwijs en onderzoek te waarborgen. Als overheid nemen we onze verantwoordelijkheid door daarbij een sterke, anticiperende rol te pakken. We willen grondrechten en publieke waarden als veiligheid en privacy beschermen. Daarom trekken we voor alle onderwijssectoren geld uit.

Het is van groot belang dat zorgvuldig met persoonsgegevens van leerlingen, studenten en medewerkers wordt omgegaan. Hoewel instellingen op de eerste plaats als «verwerkingsverantwoordelijke» zelf verantwoordelijk zijn voor het naleven van de *Algemene verordening gegevensbescherming* (AVG), moeten instellingen wel in staat zijn om dat ook te doen. Door de toenemende digitalisering in het onderwijs wordt het voor instellingen echter steeds moeilijker om de privacy te waarborgen. We gaan daarom het centraal uitvoeren van Data Protection Impact Assessments (DPIA's) op digitale producten die in het onderwijs veel gebruikt worden, faciliteren waar nodig. Daardoor kunnen instellingen beter geïnformeerde keuzes maken over de privacy van leerlingen en studenten. We sluiten daarmee aan op het advies van de Autoriteit Persoonsgegevens. Verderop in de brief kunt u er meer over lezen.

Verder werken we toe naar een gedeeld normenkader voor digitale veiligheid voor de hele sector. Het uitgangspunt daarvoor zijn de ISO27002-normen, waar het Normenkader Informatiebeveiliging in het hoger onderwijs en in het middelbaarberoepsonderwijs op is gebaseerd.[6] Het middelbaar beroepsonderwijs, het hoger onderwijs en de onderzoeksector gebruiken dat normenkader al, en zij ontwikkelen het verder. In het primair en voortgezet onderwijs bouwen we aan de invoering. Verder in de brief gaan we ook daar uitgebreider op in.

De komende tijd verkennen we hoe we verantwoording en handhaving op digitale veiligheid in het onderwijsstelsel verder kunnen inrichten. Daartoe zijn wij ook in gesprek met de Inspectie van het Onderwijs over nut en

[4] Kamerstukken 31 293, nr. 31 289 en 26 643, nr. 606.
[5] van de vaste commissie voor Onderwijs, Cultuur en Wetenschap d.d. 16 juni 2022.
[6] https://www.surf.nl/normenkader-surfaudit-audit-je-informatiebeveiliging.

noodzaak van aanvullende interventies door de inspectie. De inspectie kan binnen het huidige wettelijke kader in gesprek gaan met instellingen bij ernstige verstoringen van de continuïteit van het onderwijs, maar kent geen aparte bevoegdheden op het gebied van cyberveiligheid. Wel kan de inspectie stimulerend optreden op stelselniveau, zoals ze dat nu doet met haar sectoroverstijgende onderzoek naar cyberweerbaarheid. Als onderdeel van dat onderzoek organiseert zij onder andere ronde tafels voor bestuurders uit alle onderwijssectoren om aandacht te vragen voor de bevindingen uit het inspectierapport Binnen zonder Kloppen.

Tot slot betrekken wij, in het belang van ook die leerlingen en studenten, het niet-bekostigd onderwijs in de gesprekken en plannen voor meer digitale veiligheid. Dit gebeurt met de Nederlandse Raad voor Training en Opleiding (NRTO), de brancheorganisatie waar een groot deel van de niet-bekostigde instellingen lid van is. De NRTO investeert komende tijd aanzienlijk in het vergroten van het bewustzijn. Het NRTO trekt samen op met het Digital Trust Center (DTC) van het Ministerie van Economische Zaken en Klimaat. Leden krijgen hulp bij veilig digitaal ondernemen en informatie over preventieve maatregelen.

2. Primair en voortgezet onderwijs

De digitale veiligheid in het primair en voortgezet onderwijs moet naar een hoger niveau. Dat kan alleen met een integrale en overkoepelende aanpak waarbij in de sector en op schoolniveau alle noodzakelijke aandacht is voor het identificeren van risico's, het nemen van beschermende maatregelen, het detecteren van incidenten, het reageren op incidenten als ze zich voordoen, en het herstellen van eventuele schade.

Wij investeren structureel € 6 miljoen euro in de digitale veiligheid van het primair en voortgezet onderwijs. Daarmee zetten we belangrijke eerste stappen in de integrale aanpak die nodig is. Dit is een andere aanpak dan voorheen: wij kiezen voor meer centrale regie waarbij we sturen op normen, scholen ondersteunen met raad en daad, en externe audits en sneller optreden het sluitstuk zijn. Alleen dan kunnen schoolbesturen hun verantwoordelijkheid voor informatiebeveiliging, privacy en continuïteit invullen. Dat is ook in lijn met het advies van de Adviesgroep Regie op ICT van de PO-Raad, de VO-raad, SIVON en Kennisnet[7]. Wij werken drie prioriteiten uit en betrekken daarbij de genoemde partijen:

1) Een normenkader voor scholen

We stellen een normenkader op voor informatiebeveiliging en privacy in het primair en voortgezet onderwijs. Doordat er nu geen normenkader is, weten scholen niet altijd wat ze moeten doen om hun systemen te beveiligen. De wereld van informatiebeveiliging is omvangrijk, specialistisch en verandert razendsnel. Ook privacymaatregelen vergen specialistische juridische kennis die niet op iedere school aanwezig is. Dat zorgt voor verschillen tussen scholen en daarmee ook voor verschillen in de digitale veiligheid van leerlingen. Daar willen we vanaf. De veiligheid van leerlinggegevens mag niet afhangen van de school waar je op zit. Voor elke school moet duidelijk zijn waar ze aan moeten voldoen om veilig digitaal onderwijs te verzorgen. Daarom werken we toe naar een verplichting van dit normenkader met extra toezicht en externe audits daarop. Daar waar scholen achterblijven en niet voldoen aan het normenkader zullen we ondersteunen waar dat kan en ingrijpen waar dat nodig is.

[7] https://www.poraad.nl/schoolontwikkeling/digitalisering/advies-waarom-regie-op-ict-geen-uitstel-duldt.

Kennisnet werkt voor ons op dit moment aan een eerste versie van het normenkader en betrekt de PO-Raad, VO-raad en SIVON daarbij. Zij nemen daarbij het normenkader van SURF, de ICT-coöperatie van het hoger onderwijs en onderzoek, als uitgangspunt en scherpen dit op ons verzoek waar nodig aan. Wij stellen het normenkader vast en verspreiden het naar alle schoolbesturen. Hiermee zetten we de stap naar een onderwijsbreed kader, dat ook voor het primair en voortgezet onderwijs goed werkt. Uitgangspunt is dat het kader veiligheid biedt voor alle leerlingen, scholen en daarmee de hele sector en dat het bruikbaar is voor grote en kleine schoolbesturen.

Op basis van het normenkader zal er begin 2023 een nulmeting worden uitgevoerd voor de hele sector. Daarmee brengen we in kaart waar elk schoolbestuur staat ten opzichte van de norm. Scholen moeten vervolgens aan de slag en wij geven scholen de ondersteuning om te voldoen aan het normenkader. Daarna zullen we met periodieke monitors en benchmarks volgen hoe schoolbesturen voldoen aan de norm zodat we weten waar scholen extra ondersteuning nodig hebben. Zo geven we uitvoering aan de toezegging om te komen tot een gedeeld normenkader ten aanzien van digitale veiligheid met sectorspecifieke uitwerking.

2) Bewustwording en professionalisering

We verplichten schoolbesturen om vanaf schooljaar 2023/2024 in hun jaarverslag expliciet aandacht te besteden aan informatiebeveiliging en privacy (IBP). Dat zorgt ervoor dat besturen doordrongen raken van hun verantwoordelijkheid ten aanzien van digitale veiligheid en privacy. Daarmee geven we uitvoering aan de toezegging hierover in het eerder genoemde Kamerdebat van 1 december 2021. Digitale veiligheid is niet alleen iets voor de ICT-verantwoordelijke, maar een verantwoordelijkheid van de hele school, van het bestuur tot en met de leraar in de klas. Daarom ondersteunen wij de professionalisering van het personeel binnen scholen, onder andere met bewustwordingscampagnes, een centraal scholingsaanbod en cybercrisisoefeningen.

3) Ondersteuning op orde

Hulp en meldplicht bij cyberincidenten

Er komt een Computer Emergency Response Team (CERT) voor het primair en voortgezet onderwijs. Het CERT werkt als een «digitale brandweer»; het is een meldpunt waar scholen zich kunnen melden wanneer ze met een incident te maken krijgen en dat scholen ondersteunt bij de afhandeling daarvan. In het primair en voortgezet onderwijs is er nog geen hulp voor scholen bij dreigingen en incidenten. Het CERT voor het primair en voortgezet onderwijs sluit zich aan bij het Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden, zodat o.a. het Nationaal Cyber Security Centrum (NCSC) informatie en advies over dreigingen en kwetsbaarheden ook met scholen kan delen. Wanneer het CERT voor het primair en voortgezet onderwijs operationeel is, zullen we daar ook een meldplicht voor cyberincidenten aan koppelen. Het is belangrijk dat scholen zich ook daadwerkelijk melden als een incident zich voordoet, niet alleen voor de scholen zelf, maar ook voor de veiligheid van de hele sector. Hiermee geven we uitvoering aan de toezegging om alle instellingen te laten aansluiten bij informatievoorziening over digitale bedreigingen.

Veilige digitale infrastructuur

De komende jaren bouwen we stap voor stap aan een digitale infrastructuur die het mogelijk maakt om risico's te identificeren, beschermende maatregelen te nemen, incidenten te detecteren, daarop te reageren en eventuele schade te herstellen. Daarbij sluiten we zo goed mogelijk aan op de behoeften van het onderwijs en op bestaande voorzieningen, zoals het Nationaal Dienstencentrum (NDC) bij Kennisnet en de dienst Veilig Internet van SIVON, en de Nederlandse Cybersecurity Strategie (NLCS). Ook doen we kennis en inspiratie op bij andere sectoren en zoeken we de samenwerking. Belangrijke voorbeelden zijn de manieren waarop het CERT en Security Operations Centre (SOC) zijn ingericht in andere sectoren zoals hoger onderwijs, gemeentelijke overheden en de zorgsector. ICTU (ICT-uitvoeringsorganisatie voor de overheid) adviseert ons daarbij.

Structurele aandacht voor privacy in het onderwijs

SIVON en SURF voeren met scholen en instellingen centrale Data Protection Impact Assessments (DPIA's) uit op de digitale producten die het meest gebruikt worden in het onderwijs. Zij werken daarbij samen met het Ministerie van Justitie en Veiligheid en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De overheid kan de verantwoordelijkheid om een DPIA uit te voeren niet van scholen overnemen, maar kan scholen wel ondersteunen bij de uitvoering daarvan. Voor een DPIA is specifieke technische en juridische kennis nodig. Deze kennis is kostbaar. Bovendien is het niet efficiënt als iedere school voor zich deze analyse laat maken op een product dat door heel veel scholen gebruikt wordt. Voordeel van de samenwerking is dat er in één keer afspraken met leveranciers gemaakt kunnen worden voor het hele onderwijs. Scholen kunnen op basis van de centrale DPIA's een eigen, schoolspecifieke DPIA opstellen. Zo kunnen ze verantwoorde afwegingen maken om de privacy van leerlingen te beschermen.

Het uitvoeren van DPIA's is bovendien van belang omdat steeds meer technologiebedrijven hun producten richten op het Nederlandse onderwijs. Uw Kamer heeft dan ook meermaals aandacht gevraagd voor de privacy van leerlingen wanneer scholen gebruikmaken van dit soort producten. SURF en SIVON vervullen een belangrijke rol in het aanspreken van leveranciers op hun verantwoordelijkheid zodat hun producten aansluiten bij de waarden van het onderwijs en de Nederlandse wet- en regelgeving, en deze op een verantwoorde manier gebruikt worden. Inmiddels zijn er meerdere DPIA's en DTIA's (Data Transfer Impact Assessments) uitgevoerd op producten en diensten van Microsoft, Google en Zoom. Die hebben geleid tot aanvullende afspraken en verbeterplannen bij deze leveranciers. Daarnaast lopen er onderzoeken en gesprekken met Google over Chrome OS en het Google Cloud Platform. Google heeft aangegeven in augustus 2023 een nieuwe versie van Chrome OS en Chrome browser gereed te willen hebben. Die versie is dan in lijn met de afspraken die in 2021 met Google gemaakt zijn over Google Workspace. SURF en SIVON zijn met Google in gesprek over de uitwerking daarvan en zijn inmiddels ook gesprekken met andere leveranciers gestart. Meer informatie over de uitkomsten van deze DPIA's vindt u op de websites van SIVON en SURF.

Tijdens de schoolsluitingen door COVID-19 heeft het onderwijs doorgang kunnen vinden door de inzet van digitale toepassingen die onderwijs op afstand mogelijk maken. Een recent onderzoek van Human Rights Watch

wijst op de privacy-risico's die daarbij bestaan.[8] Hoewel Nederland geen deel uitmaakt van de 49 landen die door Human Rights Watch zijn onderzocht, heeft ook het onderwijs in Nederland snel de overstap moeten maken naar onderwijs op afstand.

Via lesopafstand.nl hebben we scholen vanaf begin af aan gewezen op hun verantwoordelijkheid ten aanzien van privacy en hebben we ze handvatten gegeven om daar invulling aan te geven. Daarnaast hebben meer dan 400 aanbieders van digitaal lesmateriaal het Privacyconvenant ondertekend waarin is afgesproken dat leerlinggegevens nooit gebruikt mogen worden voor reclamedoeleinden. Ten slotte zijn er, zoals hiervoor al benoemd, op de meest gebruikte online platformen inmiddels DPIA's uitgevoerd aan de hand waarvan er specifieke afspraken zijn gemaakt om de privacy van leerlingen optimaal te beschermen. Daarmee handelen we in lijn met de aanbevelingen die Human Rights Watch aan overheden doet.

Met dit pakket aan maatregelen zetten we belangrijke eerste stappen in het borgen van de digitale veiligheid van alle leerlingen in het primair en voortgezet onderwijs. Voor een integrale en overkoepelende aanpak van digitale veiligheid is nog een verdere verkenning en uitwerking nodig. Te denken valt aan een veilige digitale infrastructuur voor alle scholen met snel en betrouwbaar internet en real-time dreigingsdetectie. We gaan hier de komende tijd mee aan de slag en zullen uw Kamer daarover blijven informeren.

3. Hoger onderwijs, middelbaar beroepsonderwijs en onderzoek

In de kamerbrief van 28 september 2021 zijn maatregelen en afspraken aangekondigd om de digitale veiligheid van de onderwijs- en onderzoeksector te vergroten.[9] Op basis daarvan hebben de koepels plannen van aanpak opgesteld. De MBO-Raad, de Vereniging van Hogescholen (VH), de Universiteiten van Nederland (UNL) en de NRTO doen het volgende voor het verhogen van hun digitale veiligheid.

1) Vergroten bewustzijn

De instellingen vergroten het bewustzijn van digitale veiligheid bij studenten, medewerkers en bestuurders. Zo agendeert de Stuurgroep Bedrijfsvoering en Financiën (SBF) van de universiteiten digitale veiligheid minimaal tweemaal per jaar. De Vereniging Hogescholen heeft een focusgroep integrale veiligheid en bespreekt het thema een aantal keer per jaar.

De instellingen in het hoger- en middelbaar beroepsonderwijs zijn nauw betrokken bij de producten en campagnes van SURF. Docenten krijgen hulp van SURF bij de bij de inzet van educatieve tools. MBO Digitaal stimuleert de deelname aan awareness-programma's en kennisdeling via het Netwerk IBP.[10]

---

[8] https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments.

[9] Kamerstukken 31 288, nr. 31 524 en 26 643, nr. 922.

[10] MBO Digitaal was voorheen Sambo-ICT. Het netwerk IBP (Informatiebeveiliging en privacy) wordt gefaciliteerd door MBO digitaal.

2) Borgen risicomanagement

De koepels hebben de ambitie uitgesproken dat alle instellingen zich aansluiten op een Security Operations Center (SOC).[11] Vervolgens kan informatie via SURFcert over dreiging snel gedeeld worden met andere instellingen, zodat ze preventieve maatregelen kunnen treffen. Een groot deel van de universiteiten is inmiddels aangesloten op een SOC-oplossing. De laatste universiteiten willen nog dit jaar op een SOC-oplossing zijn aangesloten, de hogescholen in 2024. Het mbo moet nog meer stappen zetten en moet daarbij rekening houden met kleinere instellingen. Maar ook het mbo is bezig zich aan te sluiten op een SOC en komt eind van dit jaar met een plan hoe alle mbo-instellingen aangesloten kunnen worden. Door samenwerking in SURF-verband kunnen instellingen gezamenlijk onderhandelen over de kosten, en de professionaliteit versterken. Dit heeft geleid tot een gezamenlijke aanbesteding en gunning van de SOC-dienst bij SURF.

Gedeeld normenkader

De instellingen in het hoger en middelbaar beroepsonderwijs gebruiken voor hun audits het Toetsingskader Informatiebeveiliging Hoger Onderwijs van SURF.[12] De ambitie is een gemiddeld Capability Matury Model (CMM) volwassenheidsniveau van 3,0 voor iedere instelling, waarbij sommige instellingen op basis van hun risicoprofiel op onderdelen een hoger volwassenheidsniveau na kunnen streven.[13] Universiteiten willen dat al in 2023 halen, de hogescholen in 2024. Het mbo start in 2022 met het nieuwe toetsingskader en trekt samen op met het hoger onderwijs. De mbo-instellingen hebben meer tijd nodig om het ambitieniveau te halen. Een realistisch tijdpad wordt de komende maanden uitgewerkt. Om de mbo-instellingen hierin te ondersteunen investeren we de komende vijf jaar jaarlijks 5 miljoen euro in het verhogen van de digitale weerbaarheid.

Interne & externe audits

Alle universiteiten lieten in 2020–2021 een externe audit uitvoeren op de informatiebeveiliging. Ze hebben afgesproken dat jaarlijks te herhalen. Hogescholen willen minimaal iedere twee jaar een externe audit af laten nemen. De mbo-instellingen voeren jaarlijks assessments uit voor de benchmark IBP-E waarbij zij ofwel gebruik maken van externe auditors of werken met peer-reviews. De mbo-instellingen kijken of met het hoger onderwijs en SURF een sectorbrede aanpak opgezet kan worden. Dat kan de kosten drukken en de kwaliteit van de audits verhogen.

Verantwoording

Om de voortgang op de maatregelen te monitoren, voeren we tweemaal per jaar met de koepels in het beroepsonderwijs en het hoger onderwijs en de instituten van NWO en KNAW een bestuurlijk overleg. In deze jaarlijkse cyclus presenteren de koepels in het voorjaar het sectorbeeld van het voorgaande jaar, onder andere gebaseerd op de audituitkomsten. In het najaar rapporteren de koepels over de sectorale voortgang en de

[11] Een SOC-oplossing zorgt voor de continue monitoring van netwerken en de signalering van dreigingen.

[12] Normenkader informatiebeveiliging hoger onderwijs kent zes clusters met elk een eigen volwassenheidsniveau. In de laatste SURFaudit van 2019 was de gemiddelde score van alle instellingen op de zes onderdelen 2,3. Het afgesproken gemiddeld CMM volwassenheidsambitieniveau is 3.

[13] Capability, Maturity Model (CMM).

benodigde financiële, technische en personele investeringen om de doelstellingen te behalen. Naar aanleiding hiervan spreken we dan af met universiteiten, hogescholen en mbo-instellingen welke elementen van de digitale veiligheidsaanpak ze in het jaarverslag opnemen.

In de plannen van aanpak benadrukken de koepels dat de Raden van Toezicht zowel bij cyberincidenten en de nasleep ervan als in het monitoren van de cyberweerbaarheid van hun instelling een belangrijke rol hebben. Hiermee wordt gehoor gegeven aan de eerdere oproep van voormalig Minister van OCW om cyberveiligheid als onderwerp structureel met de Raden van Toezicht te bespreken. Om hun expertise te vergroten organiseerde UNL in de eerste helft van 2022 een trainingssessie voor de toezichthouders, over hun rol voor, tijdens en na incidenten. De Vereniging van toezichthouders van hogescholen hield verschillende sessies voor haar leden over digitale veiligheid en de lessen die geleerd zijn van incidenten. Dit blijven ze ook komend jaar doen. Ook het mbo organiseerde informatiesessies.

3) Ketensamenwerking

Bij een effectieve bestrijding van risico's bestaat de samenwerking ook uit een continue kennis- en informatiedeling over deze risico's. Universiteiten en hogescholen, mbo-instellingen en onderzoeksinstellingen delen evaluaties na incidenten en goede voorbeelden. Ze doen dat binnen hun eigen sectoren, maar ook in SURF-verband. NWO en KNAW zijn bij die kennisuitwisseling betrokken.

De instellingen stellen via SURF gezamenlijke eisen aan leveranciers en regelen gezamenlijk aanbestedingen van veilige software. Hogescholen vermijden schaduwsoftware en kopen hun software in volgens veiligheidsrichtlijnen. Ook software- en examenleveranciers doen mee. De koepels willen gezamenlijk optrekken om de veiligheid te garanderen, onder andere met gezamenlijke audits en tests waarbij gekeken wordt hoe diep hackers in het systeem door kunnen dringen.

Ook in internationaal verband is kennis-en informatiedeling relevant en heeft ook de overheid hier een verantwoordelijkheid in. Bijvoorbeeld door de sector van informatie te voorzien en te ondersteunen bij Europese wet- en regelgeving, zoals de herziening van de NIS2 richtlijn.[14] Dit geldt ook voor informatie over dreigingen die komt van het Nationaal Cyber Security Centrum (NCSC) en de inlichtingendiensten.

Privacybescherming van studenten

De mbo-instellingen coördineren al enige jaren zelf de samenwerking over privacybescherming in het mbo. De mbo-instellingen delen kennis over privacy in het netwerk IBP en maken hun volwassenheid over privacybescherming transparant middels de IBP benchmark. In het mbo kan op basis van de meest recente scores in de IBP benchmark niet worden geconcludeerd dat alle mbo instellingen inmiddels (of binnenkort) hun privacybescherming voldoende hebben geborgd. Daarmee is er noodzaak voor ons om mbo-instellingen te helpen bij de versnelling in hun groei in volwassenheid.

[14] NIB2/NIS2 De Network and Information Security Directive regelt o.a. wettelijke verplichtingen op het gebied van cybersecurity voor de vitale infrastructuur. Deze richtlijn is de opvolger van de NIS-Directive uit 2016 en bevat het voorstel om bepaalde onderzoeksinstellingen onder de richtlijn te brengen.

Wij vertalen het advies van de AP voor coördinatie in het mbo naar het volgende; wij verzoeken de MBO Raad om regie te nemen op de totstandkoming van een sector breed plan van aanpak privacybescherming mbo en de coördinatie op de uitvoering van dat plan. Wij ondersteunen dat plan van aanpak financieel vanuit de eerder genoemde 5 miljoen euro die beschikbaar is uit het coalitieakkoord (bijlage bij Kamerstuk 35 788, nr. 77). Het plan van aanpak moet aandacht besteden aan de vier adviezen van de AP, het centraal uitvoeren van DPIA's en onze adviezen over hoe privacybescherming in het mbo naar een hoger volwassenheidsniveau kan worden gebracht.

Hoger onderwijsinstellingen werken ook aan de privacy naar aanleiding van het advies van de AP. Daarin krijgen onderwijsinstellingen ondersteuning van SURF, bijvoorbeeld met betrekking tot DPIA's. Eind mei 2022 publiceert SURF het nieuwe «SURF audit toetsingskader Privacy 2022» waarmee een pilot wordt gestart bij de bij SURF aangesloten onderwijsinstellingen, waaronder universiteiten, mbo- en hbo-instellingen. Onderwijsinstellingen kunnen hieraan deelnemen. Het toetsingskader zal door het hoger onderwijs worden gebruikt voor gegevensbeschermingsbeleid in overeenstemming met privacyregelgeving. De verwachting van SURF is dat het nieuwe toetsingskader inzicht zal geven in het privacy volwassenheidsniveau van het hoger onderwijs. Eind 2022 worden de resultaten van de pilot bekendgemaakt. Wij blijven hierover in gesprek met SURF, de VH, de UNL en de hoger onderwijsinstellingen.

Daarnaast is op 11 mei 2022 het «Referentiekader privacy en ethiek voor studiedata» voor verantwoord gebruik van studiedata gepubliceerd door het Versnellingsplan Onderwijsinnovatie met ICT. Hierin zijn gezamenlijke kaders bepaald die het zorgvuldig omgaan met studiedata en studentgegevens bevorderen. Het referentiekader is omarmd door de VH en UNL.

4. Overige toezeggingen

In het Commissiedebat van 1 december 2021 is nog een drietal toezeggingen gedaan waarover we uw Kamer ook met deze brief informeren.

1) Rekenmachines bij de centrale examens

Toegezegd was de Kamer te informeren over het gebruik van grafische rekenmachines bij de centrale examens en over alternatieven daarvoor. Het College voor Toetsen en Examens (CvTE) verkent de mogelijkheden om het hulpmiddel dat is toegestaan bij de centrale wiskunde examens havo en vwo (momenteel een aantal specifiek toegestane grafische rekenmachines) uit te breiden met software-tools. Om gelijke kansen te waarborgen wordt eerst onderzocht of het mogelijk is om een lijst van eisen op te stellen waar zo'n toegestaan hulpmiddel aan moet voldoen. Als een dergelijke lijst met eisen onvoldoende blijkt om gelijke kansen te waarborgen, als de te maken kosten voor kandidaten buitenproportioneel zijn of er geen werkbaar proces in te richten valt, beoogt het CvTE via een aanbestedingsprocedure een tool te laten ontwikkelen. Een dergelijke tool zou dan vanuit de overheid beschikbaar gesteld kunnen worden als hulpmiddel bij de centrale examens wiskunde in havo en vwo.

2) Afwegingskader online-fysiek onderwijs en de rol van de medezeggenschap

Er is ook toegezegd uw Kamer nader te informeren over het afwegingskader online-fysiek onderwijs. Op 1 juni jl. is aan uw Kamer de rapportage «Ruimte voor onderwijs tijdens corona, evaluatie servicedocumenten

corona» gestuurd.[15] De brief over het afwegingskader is op 8 juli jl. aan uw Kamer gestuurd.

3) Reactie op het Mare-artikel

Verder was toegezegd u te informeren over de achtergrond van het artikel in het Leidse universiteitsblad *Mare.* Dit blad publiceerde op 17 november 2021 een artikel over de inzet van slimme camera's (classroom scanners).[16] De Universiteit Leiden wilde zo studenten tellen. De *privacy officer* en de functionaris gegevensbescherming hadden daarvoor groen licht gegeven, maar de studenten kwamen in verzet. Daarom besloot de universiteit de camera's voorlopig uit te zetten.[17] De Universiteit Leiden zal in nauw overleg met de universiteitsraad besluiten over een vervolg. Een definitief besluit zal na het zomerreces plaatsvinden (september/ oktober 2022). Bij dat besluit worden twee rapportages over de veiligheids- en privacyaspecten meegenomen. Tot die tijd blijven de camera's uitgeschakeld.

Tot slot

Wij bouwen met de sectoren verder aan een veilige digitale omgeving. Dit met als doel om de continuïteit en kwaliteit van onderwijs en onderzoek te borgen. De noodzakelijke stappen die moeten worden gezet, vragen veel inzet van de instellingen. Wij hebben er vertrouwen in dat de sectoren de komende jaren de noodzakelijke omslag gaan maken. We gaan de instellingen daarbij ondersteunen door zoveel mogelijk gezamenlijk op te trekken en waar nodig sectorspecifieke maatregelen te nemen. Wij zullen de ontwikkelingen nauwgezet volgen en Uw Kamer op de hoogte brengen over de voortgang.

De Minister van Onderwijs, Cultuur en Wetenschap,
R.H. Dijkgraaf

De Minister voor Primair en Voortgezet Onderwijs,
A.D. Wiersma

[15] Kamerstukken 31 524 en 31 288, nr. 507.
[16] https://www.mareonline.nl/achtergrond/opeens-hangen-er-overal-slimme-cameras-en-die-zien-alles/.
[17] https://www.mareonline.nl/nieuws/universiteit-erkent-fouten-cameras-blijven-uit-tot-maart/.