

Veiligheidsmaatregelen op universiteiten

Wat mag de universiteit doen?

Stichting PILP

Keizersgracht 177
1016 DR Amsterdam
Nederland

Contact

T +31(0)20 261 0191
M contact@pilp.nu
W pilp.nu

Registratie

KvK 88508536
RSIN 864659246

PiLP de juridische
bondgenoot

Inhoudsopgave

Wat mag de universiteit doen?	1
Inhoudsopgave	2
1. Inleiding	3
2. Executive Summary	4
3. (Juridisch) kader	5
3.1 Universiteitsdemocratie	5
3.2 Grondrechten	6
3.3 Privacyregels op universiteiten	7
3.4 Bevoegdheden universiteiten	11
4. Identificatie studenten	14
4.1 Het vragen van een identiteitsbewijs of studentenpas buiten tentamens	14
4.2 Het fotograferen van een identiteitsbewijs of studentenpas.....	16
5. Observatie studenten.....	17
5.1 Het doorzoeken van tassen.....	17
5.2 Het maken van foto's en video's van studenten tijdens bijeenkomsten.....	19
5.3 Het inzetten van beveiliging in burger	21
5.4 Het lezen van e-mails van studenten en werknemers.....	22
6. Conclusie	23

1. Inleiding

Het afgelopen jaar rapporteerden verschillende media over (nieuwe) vergaande veiligheidsmaatregelen die verschillende Nederlandse universiteiten inzetten.¹ Zo zijn er berichten over het inzetten van beveiliging in burger, het (heimelijk) controleren van tassen, het vragen en fotograferen van identiteitsbewijzen en studentenpassen, en meer. Stichting PILP (“PILP”) krijgt veel vragen van studenten en medewerkers van verschillende universiteiten of deze nieuwe veiligheidsmaatregelen in lijn zijn met het recht. Op deze vragen ziet het huidige rapport.

De universiteit zou een open en veilige plek moeten zijn voor iedereen waar discussie en uitwisseling van ideeën vrij kunnen plaatsvinden. Bovendien vormen het universiteitsbestuur, de studenten en de medewerkers samen de universiteitsdemocratie, waarbij een vertrouwens- en samenwerkingsband tussen deze groepen zou moeten bestaan. PILP krijgt echter steeds meer meldingen binnen dat universiteiten vergaande maatregelen opleggen in het kader van de veiligheid op de universiteit, waarbij verschillende rechten en vrijheden in het gedrang kunnen komen, zoals de vrijheid van meningsuiting, vergadering en vereniging, en privacyrechten.

In een onderzoek dat in januari 2024 werd gepresenteerd over de bescherming van persoonsgegevens in het onderwijs, vat de Autoriteit Persoonsgegevens (“AP”) de onderliggende problematiek ten aanzien van gegevensverwerking op universiteiten samen:

“Onderwijsinstellingen vervullen een belangrijke maatschappelijke taak en staan middenin de samenleving. Onderwijs gaat immers niet alleen over het overbrengen van kennis; onderwijsinstellingen krijgen ook te maken met maatschappelijke kwesties. Bij steeds meer kwesties wordt verwacht dat zij daarop acteren. Voorbeelden daarvan zijn het psychisch welzijn van leerlingen en studenten, veiligheid, armoede, kansen(on)gelijkheid, polarisatie en het terugdringen van verzuim.

Ondanks deze verwachtingen en de vaak goedbedoelde intenties, is de vraag of er een AVG-grondslag is voor onderwijsinstellingen als zij persoonsgegevens (verder) verwerken voor bovengenoemde doeleinden, omdat de taak van onderwijsinstellingen op deze punten vaak (nog) niet duidelijk is omschreven in de wet. Zeker wanneer het gaat over zeer gevoelige persoonsgegevens, die onderwijsinstellingen soms registreren en delen met (publieke) organisaties. De AP ziet dat onderwijsinstellingen niet altijd goed analyseren of dit soort gegevensverwerkingen mogen en zo ja, onder welke voorwaarden. Daarnaast is het de rol van de wetgever om zo nodig voor nieuwe wetgeving te zorgen.”²

Ook beschrijft een bestuurslid van de AP wat het belang is van het zorgvuldig omgaan met gegevens van studenten en het surveilleren van deze groep:

“Van de zandbak tot de collegebank: het onderwijs is de springplank om vorm te geven aan je leven. Te ontdekken wie je bent en je dromen waar te maken. En dat met behoud van de normen en waarden die we belangrijk vinden. Het serieus nemen van de privacy van leerlingen, studenten en onderwijspersoneel is daarbij essentieel, zodat het onderwijs ook daadwerkelijk de plek is waar je je vrij en beschermd kunt ontwikkelen.”³

Omdat er weinig specifieke regelgeving is die ziet op welke veiligheidsmaatregelen universiteiten mogen treffen, legt dit rapport verschillende (juridische) kaders naast elkaar om te beoordelen of de huidige maatregelen juridisch stand kunnen houden. In het eerste deel van dit rapport zullen de meer algemene kaders besproken worden van de universiteitsdemocratie, de mensenrechten, privacyregels in het algemeen op universiteiten en de interne bevoegdheden van universiteiten om veiligheidsmaatregelen te treffen. Bij dit laatste punt zullen

¹ Zie onder andere <https://www.nporadio1.nl/nieuws/binnenland/c71eb16b-79a3-40eb-9d6e-30f9c6bb7b91/studenten-bezorgd-om-veiligheidsmaatregelen-universiteiten-observatiecultuur>; <https://nos.nl/artikel/2535105-veiligheidsmaatregelen-amsterdamse-universiteiten-bij-opening-academisch-jaar>; <https://www.ad.nl/binnenland/snap-het-verdriet-maar-veiligheid-staat-voorop-universiteit-utrecht-spreekt-zich-uit-over-protesten~a1f77851/>

² Autoriteit Persoonsgegevens 24 januari 2024, ‘Sectorbeeld Onderwijs’, p. 2. URL: <https://www.autoriteitpersoonsgegevens.nl/documenten/sectorbeeld-onderwijs-2021-2023>

³ Autoriteit Persoonsgegevens 2024, p. 4.

zowel de medezeggenschapsstructuren op universiteiten als verschillen tussen private en publieke universiteiten worden meegenomen.

In het tweede deel van dit rapport wordt ingegaan op enkele specifieke maatregelen waar PILP veel vragen over heeft gekregen. Deze maatregelen zien op identificatie van studenten door middel van het vragen naar en fotograferen van identiteitsbewijzen en studentenpassen. Ook zien de maatregelen op observatie van studenten door het doorzoeken van tassen, het maken van foto's en video's van studenten, het inzetten van beveiliging in burger en het lezen van e-mails van studenten en werknemers.

PILP heeft ook zorgwekkende geluiden gehoord over discriminatie en etnisch profileren door beveiligingsmedewerkers op universiteiten. Zo zouden studenten van bepaalde etniciteit vaker onderwerp zijn van de genoemde veiligheidsmaatregelen, alsook leden en bezoekers van organisaties en evenementen van bepaalde politieke affiniteit. Universiteiten zouden nooit aan etnisch profileren of discriminerende praktijken moeten doen. Een verder onderzoek naar deze praktijken valt buiten het huidige rapport omdat de legaliteit hiervan geen onderwerp van discussie is.

2. Executive Summary

Er zijn verschillende kaders van toepassing op de veiligheidsmaatregelen die verschillende universiteiten toepassen. Een eerste kader is dat van de universiteitsdemocratie. Ook op de universiteit moeten studenten gebruik kunnen maken van hun grondrechten en de universiteit moet, meer dan andere private partijen, de grondrechten van studenten respecteren.

Veiligheidsmaatregelen kunnen een *chilling effect* hebben op verschillende grondrechten, zoals de vrijheid van meningsuiting, vergadering en vereniging. Dit omdat studenten die geobserveerd worden zich niet vrij voelen om hun mening te uiten of bepaalde bijeenkomsten te bezoeken. Ook privacyrechten kunnen door de maatregelen in het gedrang komen. Bovendien kunnen de maatregelen het recht op privéleven in het algemeen raken.

Universiteiten zijn gebonden aan de Algemene verordening gegevensbescherming ("AVG"). Dit betekent onder meer dat de verwerking van persoonsgegevens door universiteiten (inclusief het verzamelen hiervan) moeten voldoen aan verschillende eisen. Zo moet iedere gegevensverwerking een grondslag uit de AVG hebben en moet iedere verwerking een gerechtvaardigd doel dienen. Verder mogen universiteiten niet meer gegevens verwerken dan noodzakelijk voor dit doel. Studenten hebben op grond van de AVG inzagerechten en bezwaarrechten.

Universiteiten moeten voldoen aan bepaalde regels uit de Wet op het hoger onderwijs en wetenschappelijk onderzoek ("WHW") op het gebied van medezeggenschap. Afhankelijk van het type universiteit, hebben de universiteitsraad of de ondernemingsraad op bepaalde onderwerpen instemmings- of adviesrecht. Deze structuur kan impact hebben op de legaliteit van de nieuwe maatregelen: het is niet altijd duidelijk of de maatregelen via de juiste route tot stand zijn gekomen.

Verder bestaan er verschillen tussen openbare en bijzondere universiteiten, specifiek op het gebied van medezeggenschap. Bijzondere universiteiten zijn echter ook gebonden aan de AVG en andere relevante wetgeving.

Buiten inschrijving of tentamens, lijkt het vragen van een officieel identiteitsbewijs door de universiteit niet gerechtvaardigd of noodzakelijk en zou moeten kunnen worden volstaan met het vragen van de studentenpas. Het veelvuldig of onnodig vragen van een identiteitsbewijs of studentenpas kan een *chilling effect* hebben op het uitoefenen van grondrechten zoals het demonstratierecht. Universiteiten zouden dit dus alleen moeten doen als het noodzakelijk is. Het fotograferen van een identiteitsbewijs door de universiteit is vrijwel nooit toegestaan. Het fotograferen van een studentenpas is onderhavig aan de AVG en mag alleen als hier een AVG-grondslag voor is, het een gerechtvaardigd doel dient en geen minder ingrijpend middel mogelijk is.

Het doorzoeken van tassen is een ingrijpend controlemiddel die een grote impact kan hebben op het recht op privéleven van studenten. Universiteiten zouden dit alleen zeer beperkt moeten doen en alleen als er goede

redenen voor zijn. Het geheim controleren van tassen is onderworpen aan extra vereisten en zou alleen moeten gebeuren bij een redelijke verdenking van strafbaar handelen.

Het maken van foto's en video's van studenten tijdens bijeenkomsten valt onder het verzamelen van persoonsgegevens en is daarmee onderhavig aan de AVG. De universiteit heeft hiervoor een grondslag en gerechtvaardigd doel nodig. Het is onduidelijk of de universiteiten dit hebben. Verder zou dit beeldmateriaal als bijzondere persoonsgegevens gekwalificeerd kunnen worden omdat de politieke voorkeur van studenten hieruit kan worden afgeleid. In dat geval is het verzamelen hiervan verboden en lijkt de universiteit niet onder één van de uitzonderingsgronden te vallen. Hiernaast heeft dit een groot *chilling effect* op studenten. Ook is niet inzichtelijk wat de universiteit doet met het beeldmateriaal en hoe lang zij dit bewaart. Deze praktijk lijkt niet in de lijn met de AVG.

Het inzetten van beveiliging in burger is ook onderworpen aan strenge regels. Ten eerste mag beveiliging alleen in burger, en dus niet in uniform, opereren, als de universiteit hier een ontheffing voor heeft. Het is niet duidelijk of de universiteiten deze ontheffing hebben. Ten tweede is het de vraag of universiteiten voldoen aan de strenge vereisten voor heimelijke controle.

Ook het (geheim) controleren van e-mails van studenten en/of werknemers moet voldoen aan strenge vereisten voordat dit toegestaan is. Het is niet duidelijk of de universiteiten aan deze vereisten voldoen. Continue geheime controle van e-mailverkeer is in ieder geval niet toegestaan. Hiernaast is het de vraag of het controleren van e-mails van studenten überhaupt is toegestaan, aangezien de redenen voor controle die opgaan voor werknemers (zoals controleren of de werkmail niet (te veel) gebruikt wordt voor privédoeleinden (tijdens werk)), niet opgaan voor studenten. Ook hebben studenten geen arbeidscontractuele verplichtingen ten aanzien van de universiteit.

In conclusie zijn er veel vraagtekens en kanttekeningen te plaatsen bij sommige (nieuwe) veiligheidsmaatregelen van verschillende universiteiten. Met name op het gebied van privacyrechten is zeer de vraag of de universiteit wel een grondslag heeft voor de gegevensverwerkingen die zij uitvoert, en of de gegevensverwerking wel een gerechtvaardigd doel dient en noodzakelijk is. Ook op het gebied van transparantie en informatievoorziening lijken de universiteiten niet te voldoen aan hun verplichtingen onder de AVG. Voor een groot deel van de maatregelen is onduidelijk waarom de universiteiten ze uitvoeren en op welke manier, wat zij met de vergaarde informatie doen en of de maatregelen op de correcte wijze tot stand zijn gekomen in het kader van medezeggenschap. Studenten hebben het recht om te weten welke informatie over hun verzameld wordt en waarom. Ook hebben zij het recht om op de universiteit te zijn, deel te nemen aan de universiteitsdemocratie en (anoniem) vreedzame bijeenkomsten en demonstraties bij te wonen. Een deel van het huidige beleid op verschillende universiteiten heeft een *chilling effect* op verschillende mensenrechten en lijkt niet in lijn met privacywetgeving.

3. (Juridisch) kader

3.1 Universiteitsdemocratie

Studenten betalen collegegeld om op de universiteit aanwezig te zijn, zijn vaak voor langere tijd verbonden aan de universiteit en hebben een wettelijk recht op medezeggenschap en inspraak in het beleid van de universiteit.⁴ Zodoende maken zij deel uit van de universiteitsdemocratie. Het samenwerkingsverband Universiteiten van Nederland legt uit dat het idee achter bijvoorbeeld het instemmingsrecht van de medezeggenschap op hoofdlijnen van de begroting van de universiteit is dat 'als studenten meer moeten investeren voor hun studie, zij ook meer invloed moeten krijgen op de besteding van publieke onderwijsmiddelen'.⁵ Bovendien worden de leden van de medezeggenschap democratisch verkozen, waarbij iedere student een stem heeft.

⁴ Waar in het verleden hard voor is opgekomen om deze rechten te krijgen, zie bijvoorbeeld <https://www.nationaalarchief.nl/beleven/onderwijs/bronnenbox/ontruiming-van-het-maagdenhuis-1969>.

⁵ Universiteiten van Nederland, 'Hoe werkt medezeggenschap aan de universiteit', <https://www.universiteitenvannederland.nl/hoe-werkt-medezeggenschap-aan-de-universiteit> (laatst bezocht: 28/11/2024).

Deze context kleurt de manier waarop de universiteit om dient te gaan met de (grond)rechten van haar studenten. Eerder heeft PILP bijvoorbeeld beargumenteerd dat het demonstratierecht vanwege de universiteitsdemocratie verder reikt op het terrein van universiteiten dan op andere privéterreinen.⁶ Meer dan tussen andere private partijen zou tussen de universiteit en de student horizontale werking uit moeten gaan van grondrechten. Onderwijsinstellingen mogen, binnen de kaders van de wet, veiligheidsmaatregelen nemen op hun terrein. Hierbij moeten ze echter rekening houden met de fundamentele rechten van hun studenten, en deze niet ongerechtvaardigd of disproportioneel beperken.

3.2 Grondrechten

Het is duidelijk dat sommige maatregelen op universiteiten, zoals het fotograferen van identiteitsbewijzen en studentenpassen, mogelijk de privacyrechten van studenten raken. Deze maatregelen kunnen er echter ook voor zorgen dat studenten beperkt worden in de uitoefening van andere grondrechten, zoals de vrijheid van meningsuiting, vergadering en vereniging.

Deze grondrechten en vrijheden zijn neergelegd in verschillende mensenrechtenverdragen, zoals het Europees Verdrag voor de Rechten van de Mens (“EVRM”), het Internationaal Verdrag inzake burgerrechten en politieke rechten (“IVBPR”) en het Handvest van de grondrechten van de Europese Unie (“Handvest Grondrechten EU”). Ook zijn deze grondrechten neergelegd in de Grondwet.

(Heimelijke) observatie van studenten kan een *chilling effect* (afschrikwekkende werking) hebben op de uitoefening van deze rechten, met name als identificatie en observatie voornamelijk en stelselmatig worden ingezet bij politieke evenementen en bijeenkomsten van politieke organisaties die actief zijn op de universiteit. Zo overweegt het VN-Mensenrechtencomité dat surveillance een *chilling effect* kan hebben op het demonstratierecht:

“While surveillance technologies can be used to detect threats of violence and thus to protect the public, they can also infringe on the right to privacy and other rights of participants and bystanders and have a chilling effect.”⁷

Amnesty International Nederland (“AIN”) kwam tot een vergelijkbare conclusie in een recent rapport:

“Surveillance kan mensen ontmoedigen om deel te nemen aan demonstraties uit angst om gemonitord te worden.”⁸

En ook Bart Schermer, hoogleraar Recht en Digitale Technologie aan de Universiteit Leiden concludeert “Als je de hele tijd in de gaten wordt gehouden, kun je niet meer vrij demonstreren”.⁹ Universiteiten moeten zich bewust zijn van deze gevolgen en ze meenemen in de inschattingen en beoordelingen die zijn maken van de maatregelen die ze in willen zetten.

De AP benadrukt een vergelijkbaar punt in een onderzoek naar de impact van online onderwijs en proctoring op privacyrechten van studenten: er moet niet alleen gekeken worden naar de privacyrechten maar er moet ook rekening gehouden worden ‘met risico’s die raken aan andere (grond)rechten en vrijheden dan alleen het recht op bescherming van persoonsgegevens’.¹⁰

⁶ PILP, ‘Analyse ‘Richtlijn protesten universiteiten en hogescholen’ en het demonstratierecht’. Te raadplegen via:

<https://pilp.nu/juridische-analyse-demonstrerenop-universiteiten-en-hogescholen/>

⁷ VN Mensenrechtencomité, ‘General comment No. 37(2020) on the right of peaceful assembly (article 21)’, 17 september 2020, CCPR/C/GC/37, para. 10.

⁸ Amnesty International Netherlands, ‘In beeld bij de politie: Camerasurveillance bij vreedzaam protest in Nederland’, oktober 2024, p. 3. URL: <https://www.amnesty.org/en/documents/eur35/8469/2024/en/>

⁹ D. van Benthem e.a., ‘Demonstratierecht in de knel’, Investico 22 maart 2023, URL:

<https://www.platforminvestico.nl/onderzoeken/onderzoek-demonstratierecht-in-de-knel>

¹⁰ Autoriteit Persoonsgegevens oktober 2020, ‘Onderzoek online (video)bellen en online proctoring in het onderwijs’, p. 3. URL: <https://www.autoriteitpersoonsgegevens.nl/documenten/onderzoek-online-videobellen-en-online-proctoring-in-het-onderwijs>

Hoewel de bescherming van mensenrechten primair de taak is van overheden, voeren universiteiten een wettelijk opgedragen publieke taak uit¹¹ en maken studenten deel uit van de universiteitsdemocratie. Om deze redenen zou er horizontale werking moeten zijn van mensenrechten zoals het demonstratierecht tussen de universiteit en de student.¹² Inperkingen van deze rechten zouden dan ook noodzakelijk, proportioneel en subsidiair moeten zijn.¹³

Op het gebied van privacy zijn alle overheidsinstanties, bedrijven en personen in Nederland gebonden aan de AVG.¹⁴ Hierin zijn de criteria van noodzakelijkheid, proportionaliteit en subsidiariteit specifiek uitgewerkt voor inperkingen van het recht op privacy. Ook universiteiten zijn gebonden aan de AVG. Wat dit betekent voor universiteiten wordt in het volgende hoofdstuk nader toegelicht.

Naast privacyrechten in de zin van gegevensverwerking en de AVG, kunnen verschillende maatregelen ook aan het recht op privéleven van studenten in het algemeen, in de zin van artikel 8 EVRM, raken. Het EHRM heeft over verschillende maatregelen die overheden inzetten om burgers te surveilleren, overwogen dat deze een schending van het privéleven van deze burgers op kunnen leveren.¹⁵

3.3 Privacyregels op universiteiten

Veel van de maatregelen die we in dit rapport bespreken raken aan de privacyrechten van studenten en medewerkers. Het algemene juridische kader dat ziet op de verwerking van persoonsgegevens is dus relevant voor de beoordeling van de legaliteit van deze maatregelen. Overkoepelend zijn deze regels neergelegd in de AVG. Universiteiten moeten, net zoals andere organisaties in Nederland, voldoen aan de regels uit de AVG. Deze regels zijn verder uitgewerkt in de Uitvoeringswet Algemene verordening gegevensbescherming (“**UAVG**”).

De AVG stelt 6 basisprincipes op voor de verwerking van persoonsgegevens (inclusief het verzamelen hiervan)¹⁶: (i) rechtmatigheid, behoorlijkheid en transparantie (ii) doelbinding (iii) daalminimalisatie (iv) juistheid (v) opslagbeperking en (vi) vertrouwelijkheid en integriteit.¹⁷ Hierbij is het aan de verwerkende entiteit om aan te tonen dat deze beginselen nageleefd worden.¹⁸ Dit heet de verantwoordingsplicht en deze ligt in de context van dit rapport bij de universiteiten.¹⁹

De AP licht toe hoe organisaties kunnen voldoen aan de verantwoordingsplicht. Zo moeten organisaties verplicht een verwerkingsregister bijhouden²⁰, een Data protection impact assessment (“**DPIA**”) uitvoeren ‘bij

¹¹ Namelijk het verzorgen van wetenschappelijk onderwijs, het uitvoeren van wetenschappelijk onderzoek en kennisoverdracht ten behoeve van de maatschappij (artikel 1.3 WHW).

¹² In de analyse over het demonstratierecht op onderwijsinstellingen wordt eenzelfde conclusie getrokken (PiLP, ‘Analyse ‘Richtlijn protesten universiteiten en hogescholen’ en het demonstratierecht’. Te raadplegen via: <https://piip.nu/juridische-analyse-demonstrerenop-universiteiten-en-hogescholen/>)

¹³ Zoals neergelegd in mensenrechtenverdragen zoals het EVRM, IVBPR en het Handvest Grondrechten EU.

¹⁴ Deze privacyrechten zijn ook vastgelegd in de internationale mensenrechtenverdragen.

¹⁵ Zie bijvoorbeeld over geheime surveillance in het algemeen, en de wettelijke waarborgen die hierbij nodig zijn EHRM 20 juli 2021, app. nos. 58361/12, 25592/16, 27176/16 (*Zoltán Varga vs. Slowakije*), r.o. 151. En over dat het surveilleren van telefoongesprekken een inbreuk kan maken op artikel 8 EVRM, EHRM 12 januari 2023, app. no. 7286/16 (*Potocká en Adamčo vs. Slowakije*), r.o. 69. Ook het onderwerpen van een persoon aan ‘stop and search’ acties door de politie kan een inbreuk op het privéleven opleveren (EHRM 14 januari 2021, app. no. 59648/13 (*Vig vs. Hongarije*), r.o. 49).

¹⁶ De verwerking van persoonsgegevens voor persoonlijk gebruik valt niet onder de AVG.

¹⁷ Artikel 5 lid 1 AVG, samengevat door de AP (<https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/de-avg-in-het-kort#:~:text=Door%20de%20Algemene%20Overordening%20gegevensbescherming,kunnen%20zij%20een%20boete%20krijgen.>)

¹⁸ Artikel 5 lid 2 jo. artikel 24 AVG.

¹⁹ En mogelijk bij private beveiligingsbedrijven die ingezet worden door de universiteiten.

²⁰ Artikel 30 AVG.

gegevensverwerkingen met een hoog privacyrisico²¹; een datalekregister bijhouden; aantonen ‘dat een betrokkene daadwerkelijk toestemming heeft gegeven voor een gegevensverwerking wanneer u voor deze verwerking toestemming nodig heeft’; onderbouwen waarom er wel of niet een Functionaris Gegevensbescherming (“FG”) is aangesteld²² en een privacyverklaring opstellen.²³

De universiteit is ook verplicht om een verwerkingsovereenkomst aan te gaan met een verwerker als in opdracht gegevens worden verwerkt door een derde partij.²⁴ Dit zou van belang kunnen zijn bij het inzetten van beveiligers van private bedrijven. Hiernaast moet de FG betrokken worden bij alle processen omtrent de bescherming van persoonsgegevens.²⁵

Voor sommige organisaties is het ook verplicht om een privacybeleid te hebben (naast de privacyverklaring, die altijd verplicht is). Dit hangt af van de aard, omvang, context en het doel van de gegevensverwerking.²⁶ Uit dit beleid moet blijken hoe de organisatie voldoet aan de AVG.²⁷

De AP signaleerde in 2024 dat de meeste onderwijsinstellingen wel een algemene privacyverklaring hebben (zoals verplicht) en een privacyreglement, maar dat deze ‘niet altijd alle verwerkingen van de onderwijsinstelling’ bevatten.²⁸ Hierbij merkt de AP op dat er vanuit studenten een wens is ‘om meer inzicht te krijgen in wie er toegang heeft tot hun gegevens, en hier invloed op te kunnen uitoefenen’.²⁹

Verder moet een universiteit een verwerkingsregister bijhouden.³⁰ In dit register staat bepaalde informatie, zoals de doeleinden waarvoor persoonsgegevens verwerkt worden. Ook bevat dit register een beschrijving van de (categorieën van) personen van wie gegevens worden verwerkt en categorieën van persoonsgegevens die worden verwerkt.³¹ Ook bevat het register de datum waarop de gegevens gewist moeten worden en de ontvangers van de persoonsgegevens, alsmede hoe de persoonsgegevens beschermt worden.³²

Om aan het eerste beginsel te voldoen, rechtmatigheid, moet de verwerking van persoonsgegevens gebaseerd zijn op één van de grondslagen uit de AVG. De grondslagen zijn: (i) toestemming (ii) noodzakelijk ter uitvoering van een overeenkomst (iii) noodzakelijk wegens wettelijke plicht (iv) noodzakelijk om vitale belangen te beschermen (v) noodzakelijk op een taak van algemeen belang uit te voeren/openbaar gezag uit te oefenen (vi)

²¹ De universiteit is verplicht om de DPIA voorafgaand aan bepaalde verwerkingen te doen. Dit gaat bijvoorbeeld over ‘Grootschalig en/of systematisch gebruik van flexibel cameratoezicht’. Hierbij benadrukt de AP dat het uitvoeren van een DPIA ‘een continu proces’ is, waarbij de DPIA regelmatig herzien en opnieuw beoordeeld moet worden. De AP adviseert om hierbij regelmatig studenten, docenten en diens vertegenwoordigers in verschillende raden, naar hun mening te vragen over gegevensverwerking, ‘ook als er geen juridisch bindend advies- of instemmingsrecht geldt voor deze personen of organen’ (Autoriteit Persoonsgegevens 2020, p. 9).

²² Artikel 37 AVG.

²³ <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/verantwoordingsplicht>

²⁴ Autoriteit Persoonsgegevens 2020, p. 11.

²⁵ Autoriteit Persoonsgegevens 2020, p. 15, artikel 38 AVG.

²⁶ <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/verantwoordingsplicht>

²⁷ De AP noemt de volgende onderwerpen die hierin opgenomen zouden kunnen worden: ‘omschrijving van de categorieën persoonsgegevens die u verwerkt; een beschrijving van de doeleinden waarvoor u persoonsgegevens verwerkt. En wat de wettelijke grondslag daarvoor is’; hoe voldaan wordt aan de beginselen van verwerking van persoonsgegevens zoals het niet meer gegevens verwerken dan noodzakelijk; ‘welke privacyrechten betrokkenen hebben en hoe zij die rechten kunnen uitoefenen’; welke maatregelen de organisatie heeft genomen om de persoonsgegevens te beveiligen en hoe lang deze bewaard worden (<https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/verantwoordingsplicht>)

²⁸ Autoriteit Persoonsgegevens 2024, p. 8.

²⁹ Autoriteit Persoonsgegevens 2024, p. 8.

³⁰ Artikel 30 AVG.

³¹ <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/verantwoordingsplicht>

³² <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/verantwoordingsplicht>

noodzakelijk om gerechtvaardigde belangen te behartigen.³³ De AP raadt aan om de grondslag voor de verwerking te noemen in de privacyverklaring, het privacybeleid en in het verwerkingsregister.³⁴

Wanneer het gaat om de verwerking van bijzondere persoonsgegevens gelden extra strenge regels. Bijzondere persoonsgegevens ‘zijn gegevens die zo privacygevoelig zijn dat het een grote(re) impact op iemand kan hebben als een organisatie deze gegevens verwerkt’.³⁵ Het gaat dan bijvoorbeeld om gegevens ‘waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken’.³⁶ De verwerking van deze gegevens zijn verboden, tenzij aan één van de uitzonderingsgronden is voldaan.³⁷

Specifiek wat betreft de grondslagen op basis waarvan persoonsgegevens verwerkt kunnen worden, bepaalt de AVG dat overheidsinstanties in de kader van de uitoefening van hun taken geen beroep toekomt op de grondslag gerechtvaardigd belang³⁸: ‘Voor publiekrechtelijke onderwijsinstellingen geldt daarom dat zij bij de uitoefening van hun taken geen beroep kunnen doen op deze rechtsgrondslag’.³⁹

Wat betreft de grondslag toestemming overweegt de AP dat een student:

“vrije toestemming [moet] kunnen geven voor de verwerking van zijn of haar persoonsgegevens. Het element “vrij” impliceert dat er sprake is van werkelijke keuze en controle voor studenten. De gezagsverhouding tussen de onderwijsinstelling en studenten kan problematisch zijn voor een beroep op de grondslag toestemming. Het is immers de vraag of studenten daadwerkelijk de vrijheid hebben om toestemming te weigeren tegenover de onderwijsinstelling wanneer hier consequenties aan verboden zijn. Om te kunnen spreken van vrije toestemming dient de onderwijsinstelling in ieder geval een alternatief te bieden voor de (voorgenomen) verwerking. Indien een student bij het weigeren van toestemming geen onderwijs kan volgen of niet kan deelnemen aan een toets of tentamen, is er geen sprake van vrije toestemming. Ook het veronderstellen dat de student toestemming verleent door deel te nemen aan een digitale les of een online proctoring tentamen is geen rechtmatige toestemming in de zin van de AVG.”⁴⁰

Verder benadrukt de AP dat de onderwijsinstelling goed moet kunnen onderbouwen waarom een bepaalde grondslag is gekozen en dat de gegevensverwerking noodzakelijk is om het onderliggende doel te bereiken.⁴¹

³³ Artikel 6 lid 1 AVG. Zie voor nadere uitleg van deze grondslagen

<https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/grondslagen-avg-uitgelegd>

³⁴ <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/grondslagen-avg-uitgelegd>

³⁵ <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/grondslagen-avg-uitgelegd#speciale-regels-voor-bijzondere-persoonsgegevens>

³⁶ Artikel 9 lid 1 AVG.

³⁷ De uitzonderingsgronden voor het verwerken van bijzondere persoonsgegevens zijn volgens artikel 9 lid 2 AVG, samengevat door de AP (<https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/grondslagen-avg-uitgelegd#speciale-regels-voor-bijzondere-persoonsgegevens>): (i) uitdrukkelijke toestemming (ii) noodzakelijk om verplichtingen of specifieke rechten uit te voeren op het gebied van arbeidsrecht, socialezekerheidsrecht en socialebeschermingsrecht (iii) noodzakelijk om vitale belangen te beschermen en de persoon in kwestie is fysiek of juridisch niet in staat om toestemming te geven (iv) verwerking door een instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is (v) doelbewust openbaar gemaakte gegevens door de persoon zelf (vi) noodzakelijk voor een rechtsovername (vii) noodzakelijk voor een zwaarwegend algemeen belang (viii) noodzakelijk voor doeleinden van preventieve of geneeskundige aard (ix) noodzakelijk voor de volksgezondheid (x) noodzakelijk voor archivering of onderzoek.

³⁸ Artikel 6 lid 1 AVG.

³⁹ Autoriteit Persoonsgegevens 2020, p. 7.

⁴⁰ Autoriteit Persoonsgegevens 2020, p. 7-8.

⁴¹ Autoriteit Persoonsgegevens 2020, p. 8.

Om verder aan het eerste criterium te voldoen, moet de gegevensverwerking behoorlijk en transparant zijn. Dit houdt in dat deze niet ‘nadelig, discriminerend, onverwacht of misleidend mag zijn’ voor de betrokkene.⁴² Ook moet transparant zijn hoe en waarom de gegevens verwerkt worden.⁴³

Het tweede criterium, doelbinding, ziet er op dat organisaties bij het verwerken van persoonsgegevens altijd een gerechtvaardigd doel moeten hebben. De AP legt uit:

“Dat doel moet specifiek zijn en vooraf uitdrukkelijk zijn omschreven. Organisaties mogen dus niet alvast persoonsgegevens gaan verzamelen omdat die misschien ooit van pas gaan komen.”⁴⁴

Ook moet het doel van het verzamelen van de gegevens overeenkomen met het doel waarvoor deze verwerkt worden: “de organisatie mag de gegevens niet ineens voor een ander doel gaan verwerken”.⁴⁵

Universiteiten moeten ook niet meer data verwerken dan noodzakelijk, zoals bepaald in het vereiste van dataminimalisatie: “de verwerking van de gegevens moet passen bij het doel” en “de organisatie [mag] niet meer gegevens (...) verwerken dan noodzakelijk is om dat doel te bereiken”.⁴⁶

Criterium vier, juistheid, houdt in dat organisaties een verantwoordelijkheid hebben om te zorgen dat er geen onjuiste gegevens verwerkt worden, en dat deze geactualiseerd worden.⁴⁷ Criterium vijf, opslagbeperking, ziet op het volgende: “Organisaties moeten persoonsgegevens verwijderen zodra die niet langer nodig zijn voor het oorspronkelijke doel waarvoor ze zijn verzameld”.⁴⁸ Criterium 6, vertrouwelijkheid en integriteit, houdt in dat de gegevensverwerkingen goed beveiligd moeten zijn.⁴⁹

In het kader van de bovenstaande criteria hebben organisaties, en zo ook universiteiten, bepaalde verplichtingen. Zo hebben universiteiten een informatieplicht jegens degenen waarvan zij persoonsgegevens verwerken.⁵⁰ De universiteit moet aan de betrokkene onder andere laten weten welke persoonsgegevens zij verwerkt, voor welke doeleinden, op welke grondslag en hoe lang de gegevens bewaard worden.⁵¹ Ook zijn er situaties waarin de universiteit meer informatie moet verstrekken. Dit hangt onder andere af van of het gebruik van je gegevens redelijkerwijs te verwachten is, welke gevolgen dit gebruik heeft, en of het gaat om gevoelige gegevens.⁵² Hierbij moet de privacyverklaring waar deze informatie in staat duidelijk zijn en niet te lang, compleet en goed vindbaar.⁵³

In het kader van de informatieplicht op onderwijsinstellingen overwoog de AP eerder:

“Naast de inhoud van de informatie dient er ook aandacht te zijn voor de vorm waarin de informatie wordt verstrekt. Zeker van (minderjarige) studenten mag niet worden verwacht dat zij ingewikkeld juridisch jargon

⁴² <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/de-avg-in-het-kort#:~:text=Door%20de%20Algemene%20Overordening%20gegevensbescherming,kunnen%20zij%20een%20boete%20krijgen.>

⁴³ Ibid.

⁴⁴ Ibid.

⁴⁵ Ibid.

⁴⁶ Ibid.

⁴⁷ Ibid.

⁴⁸ Ibid.

⁴⁹ Ibid.

⁵⁰ Artikelen 12-14 AVG. De organisatie hoeft betrokkenen niet altijd te informeren over het gebruik van gegevens, bijvoorbeeld als de betrokkene al op de hoogte is, of als er sprake is van onevenredige inspanning of een zwaarwegend belang. In het eerste geval moet de universiteit zeker weten dat je op de hoogte bent

(<https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacyrechten-avg/recht-op-informatie>)

⁵¹ Artikel 13 AVG.

⁵² <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacyrechten-avg/recht-op-informatie>

⁵³ <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacyrechten-avg/recht-op-informatie>

begrijpen of lange privacystatements lezen. Onderwijsinstellingen dienen de informatie daarom op een toegankelijke manier te verstrekken.”⁵⁴

Studenten hebben ook een inzagerecht op grond van de AVG.⁵⁵ Zij hebben het recht om van de universiteit te horen of de universiteit hun persoonsgegevens verzamelt en om inzage te krijgen in de verzamelde persoonsgegevens.⁵⁶ Hiernaast hebben studenten het recht om van deze verzamelde gegevens onder andere te horen wat de verwerkingsdoeleinden hiervoor zijn, wie de gegevens ontvangen en hoe lang de gegevens bewaard zullen worden.⁵⁷

Ook hebben studenten een bezwaarrecht op grond van de AVG: zij hebben het recht ‘om bezwaar te maken tegen de verwerking van zijn of haar persoonsgegevens vanwege “met zijn specifieke situatie verband houdende redenen”’.⁵⁸ Mocht een student bezwaar maken, dan moet de gegevensverwerking door de onderwijsinstelling stoppen, ‘tenzij deze kan aantonen dat zijn dwingende gerechtvaardigde belangen zwaarder wegen dan de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene. Dit vereist dat de onderwijsinstelling een afweging maakt tussen de belangen van de student en die van de onderwijsinstelling’.⁵⁹ Het is aan de onderwijsinstelling om studenten op de hoogte te stellen van hun bezwaarrecht.⁶⁰

3.4 Bevoegdheden universiteiten

3.4.1 Medezeggenschap en bevoegdheidsstructuur

Het laatste kader dat besproken wordt voordat toegekomen wordt aan de legaliteit van specifieke maatregelen, is die van de bevoegdheidsstructuur op universiteiten. Uit het volgende deel zal namelijk blijken dat er situaties denkbaar zijn waarin bepaalde maatregelen ingezet kunnen worden door de universiteit, maar dat het zeer de vraag is of ze tot stand zijn gekomen via de correcte route. Voor sommige vergaande beslissingen heeft de universiteit namelijk instemming nodig van bepaalde medezeggenschapsraden, of mogen deze een advies uitbrengen. In het bepalen van eventuele stappen die studenten kunnen zetten om hun universiteit aan te spreken als zij menen dat hun rechten niet (voldoende) gewaarborgd worden, is dus ook relevant of de universiteit via de juiste route tot beslissingen over nieuwe veiligheidsmaatregelen zijn gekomen.

De medezeggenschap op universiteiten, en hiermee welk orgaan betrokken dient te worden bij het treffen van (vergaande) veiligheidsmaatregelen, is geregeld in de Wet op het hoger onderwijs en wetenschappelijk onderzoek (“WHW”).⁶¹ Kort gezegd zijn er twee varianten. Een universiteit kan een Universiteitsraad hebben waar zowel studenten als medewerkers in zitten. In de tweede variant heeft de universiteit een Studentenraad en een Ondernemingsraad en een gezamenlijke raad met afgevaardigde van deze twee raden.⁶²

Bijzondere universiteiten, moeten alle regels uit de WHW over medezeggenschap overnemen tenzij de aard van de universiteit zich daar tegen verzet naar het oordeel van het college van bestuur.⁶³ Ook kan de Minister van Onderwijs, Cultuur en Wetenschap op verzoek van het instellingsbestuur ontheffing verlenen van bepaalde wettelijke voorschriften uit de WHW.⁶⁴

⁵⁴ Autoriteit Persoonsgegevens 2020, p. 21.

⁵⁵ Artikel 15 AVG.

⁵⁶ Artikel 15 lid 1 AVG.

⁵⁷ Artikel 15 lid 1 AVG.

⁵⁸ Autoriteit Persoonsgegevens 2020, p. 24 over artikel 21 AVG. Dit recht hebben studenten alleen ‘als de grondslag van de verwerking is gebaseerd op ofwel de vervulling van een taak van algemeen belang of de uitoefening van het openbaar gezag (...) of het gerechtvaardigd belang’ (Autoriteit Persoonsgegevens 2020, p. 24 over artikel 21 lid 1 AVG).

⁵⁹ Autoriteit Persoonsgegevens 2020, p. 24.

⁶⁰ Autoriteit Persoonsgegevens 2020, p. 24.

⁶¹ <https://www.universiteitenvannederland.nl/hoe-werkt-medezeggenschap-aan-de-universiteit>

⁶² W. Boer 4 maart 2020, ‘Hoe werkt de medezeggenschap op universiteiten?’, Vereniging van Universiteiten. URL: <https://www.universiteitenvannederland.nl/files/publications/200224%20Hoe%20werkt%20de%20medezeggenschap%20-%20februari%202020.pdf>. Artikelen 9.30 & 9.30a WHW.

⁶³ Artikel 9:51 lid 2 WHW.

⁶⁴ <https://lsvb.nl/dossiers/medezeggenschap/rechten-van-de-medezeggenschap/>

Op grond van de WHW is de universiteitsraad bevoegd over ‘alle aangelegenheden de universiteit betreffende aan het college van bestuur voorstellen te doen en standpunten kenbaar te maken’ waarop het college van bestuur een met redenen omklede reactie moet uitbrengen.⁶⁵ Ook stelt het college de universiteitsraad op de hoogte van het gevoerde beleid en de beleidsvoornemens op onder andere organisatorisch gebied.⁶⁶ Hiernaast moet het college de universiteitsraad tijdig alle inlichtingen geven die de raad ‘voor de vervulling van zijn taak naar redelijkheid en billijkheid nodig kan hebben’.⁶⁷ Verder heeft het college van bestuur de instemming van de universiteitsraad nodig ‘voor elk door het college van bestuur te nemen besluit met betrekking tot ten minste de vaststelling of wijziging van’ het instellingsplan, het studentenstatuut en het bestuurs- en beheersreglement.⁶⁸

Hiernaast heeft de universiteitsraad adviesbevoegdheid over besluiten die betrekking hebben tot ‘aangelegenheden die het voortbestaan en de goede gang van zaken binnen de universiteit betreffen’.⁶⁹

Als de universiteit een ondernemingsraad (“OR”) heeft en het college van bestuur heeft besloten dat de Wet op de ondernemingsraden (“WOR”) van toepassing is⁷⁰, zijn in de WOR verschillende regels neergelegd wat betreft instemming en advies. Zo moet toestemming gevraagd worden aan de OR als de universiteit personeelsgegevens wil gebruiken of werknemers wil monitoren.⁷¹

Verder heeft de werkgever instemming van de OR nodig voor ‘elk door hem voorgenomen besluit tot vaststelling, wijziging of intrekking van (...) een regeling omtrent het verwerken van alsmede de bescherming van de persoonsgegevens van de in de onderneming werkzame personen’.⁷² Zulke instemming is ook nodig bij regelingen over ‘voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen’.⁷³

Hiernaast heeft de OR ook het initiatiefrecht om zich op eigen initiatief uit te spreken over het gebruik van personeelsgegevens.⁷⁴ De AP noemt als voorbeelden waarin dit recht ingezet kan worden ‘vanwege een beveiligingsincident of vragen of klachten van werknemers. Of iets anders waarbij de OR vindt dat de werkgever actie moet ondernemen’.⁷⁵ De OR kan in zo’n geval een initiatiefvoorstel doen waar de werkgever verplicht een beslissing moet nemen.⁷⁶

De OR heeft ook adviesrecht. De werkgever vraagt de OR om advies, onder andere over ‘elk door hem voorgenomen besluit tot (...) invoering of wijziging van een belangrijke technologische voorziening’.⁷⁷ Dit kan bijvoorbeeld gaan om een nieuw automatiseringssysteem of communicatiesysteem.⁷⁸

Specifiek op het gebied van personeelsvolgsystemen heeft de werkgever ook de instemming van de OR nodig. Voorbeelden van personeelsvolgsystemen zijn: ‘een systeem dat aanwezigheid, tijd en toegang registreert (...)

⁶⁵ Artikel 9.32 lid 2 WHW.

⁶⁶ Artikel 9.32 lid 5 WHW.

⁶⁷ Artikel 9.32 lid 6 WHW.

⁶⁸ Artikel 9.33 lid 1 WHW.

⁶⁹ Artikel 9.33a lid 1 sub a WHW.

⁷⁰ In de zin van artikel 9.30 lid 1 sub a WOR.

⁷¹ <https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/ondernemingsraad/de-rol-van-de-or-bij-privacy-op-het-werk>

⁷² Artikel 27 lid 1 aanhef en sub k WOR.

⁷³ Artikel 27 lid 1 aanhef en sub l WOR.

⁷⁴ Artikel 23 lid 23 WOR.

⁷⁵ <https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/ondernemingsraad/de-rol-van-de-or-bij-privacy-op-het-werk>

⁷⁶ <https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/ondernemingsraad/de-rol-van-de-or-bij-privacy-op-het-werk>

⁷⁷ Artikel 25 lid 1 aanhef en sub k WOR.

⁷⁸ <https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/ondernemingsraad/de-rol-van-de-or-bij-privacy-op-het-werk>

software die bijvoorbeeld (...) e-mailverkeer (...) van werknemers registreert; cameratoezicht op de werkplek'.⁷⁹ Voor het instellen van een dergelijk systeem moet de werkgever instemming vragen van de OR.⁸⁰ De AP benadrukt hierbij dat de OR 'óók instemmingsrecht [heeft] bij een systeem dat de werkgever (nog) niet gebruikt om werknemers te volgen, maar waarbij dit wel zou kunnen'.⁸¹ Verder is het belangrijk om een dergelijk systeem kritisch te toetsen, waarbij de FG kan adviseren over of het systeem bijvoorbeeld nodig is.⁸²

Zoals hieronder verder besproken zal worden, zijn in sommige gevallen vraagtekens gezet bij of de nieuwe veiligheidsmaatregelen van de universiteiten wel tot stand zijn gekomen in overeenstemming met dit instemmings- en advieskader.⁸³ Een reden hiervoor zou kunnen zijn is dat de maatregelen mogelijk onder (tijds)druk zijn ontstaan. De AP benadrukt echter, in een rapport over online onderwijs en proctoring tijdens de coronapandemie, dat tijdelijke maatregelen vaak toch blijvend worden ingezet, en dat daarom goed gekeken moet worden of deze maatregelen voldoen aan alle wettelijke vereisten:

"Toch heeft de AP ook gezien dat onderwijsinstellingen bij de omschakeling naar het afstandsonderwijszaken omtrent de bescherming van persoonsgegevens niet altijd voldoende in ogenschouw hebben genomen. Gelet op de hoge urgentie van deze omschakeling en de grote impact op het onderwijs is dit te begrijpen, maar de AP vindt het belangrijk dat onderwijsinstellingen hierin transparant zijn en alsnog al het redelijke inzetten om op korte termijn, daar waar nodig, de juiste waarborgen te treffen. De praktijk leert immers dat 'tijdelijke' maatregelen ook op de lange termijn blijvend worden ingezet. Daarom is het van groot belang dat bij tijdelijke oplossingen, ook als deze onder tijdsdruk moeten worden doorgevoerd, voldoende stil wordt gestaan bij de bescherming van persoonsgegevens."⁸⁴ (nadruk toegevoegd)

3.4.2 *Verschillen tussen openbare en bijzondere universiteiten*

De meeste universiteiten in Nederland zijn openbare universiteiten. Er zijn echter ook 'bijzondere' universiteiten, die door particulieren zijn opgericht in plaats van door de staat. Dit zijn de Vrije Universiteit, de Radboud Universiteit en Tilburg University.⁸⁵ Deze universiteiten zijn, zoals hierboven toegelicht, verplicht om de medezeggenschapsregelingen uit de WHW over te nemen, tenzij de aard van de universiteit zich hiertegen verzet.⁸⁶ Het kan dus zo zijn dat op de bijzondere universiteiten de medezeggenschapsraden op bepaalde onderwerpen meer of minder rechten hebben. Het valt buiten de reikwijdte van dit rapport om dit per universiteit te onderzoeken.

Verder zou beargumenteerd kunnen worden dat de privaatrechtelijke status van bijzondere universiteiten impact kan hebben op in hoeverre de mensenrechten van studenten horizontale werking toekomt en in hoeverre de universiteitsdemocratie een relevant kader is. Het valt ook buiten de reikwijdte van dit rapport om hier uitgebreid op in te gaan, voornamelijk omdat hier simpelweg geen concrete regels of consensus over bestaat. Het zou echter te ver gaan om te stellen dat er geen universiteitsdemocratie op bijzondere universiteiten bestaat: ook bijzondere universiteiten moeten medezeggenschap van studenten en werknemers regelen, waarbij deze twee groepen ook rechten hebben om betrokken te worden in deze keuzes.

Ook gaat het te ver om te concluderen dat bijzondere universiteiten de mensenrechten van hun studenten niet hoeven te respecteren. In ieder geval op het gebied van privacyregels zijn de bijzondere universiteiten ook

⁷⁹ <https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/ondernemingsraad/de-or-en-personeelsvolgsystemen>

⁸⁰ Artikel 26 lid 1 sub I WOR.

⁸¹ <https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/ondernemingsraad/de-or-en-personeelsvolgsystemen>

⁸² <https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/ondernemingsraad/de-or-en-personeelsvolgsystemen>

⁸³ <https://www.mareonline.nl/nieuws/universiteitsraad-stop-per-direct-met-beveiligers-in-burger/>

⁸⁴ Autoriteit Persoonsgegevens oktober 2020, 'Onderzoek online (video)bellen en online proctoring in het onderwijs', p. 3. URL: <https://www.autoriteitpersoonsgegevens.nl/documenten/onderzoek-online-videobellen-en-online-proctoring-in-het-onderwijs>

⁸⁵ Bijlage behorende bij de WHW, onder b.

⁸⁶ Artikel 9.51 lid 2 WHW.

gebonden aan de AVG. Veel van de hierna besproken veiligheidsmaatregelen raken aan de AVG. Deze delen gelden gelijk voor beide soorten universiteiten. Maar ook andere grondrechten, zoals het demonstratierecht, zouden gerespecteerd moeten worden door bijzondere universiteiten.

4. Identificatie studenten

4.1 Het vragen van een identiteitsbewijs of studentenpas buiten tentamens

Een eerste maatregel die (recentelijk) op universiteiten wordt ingezet, is het vragen van een identiteitsbewijs of studentenpas aan studenten. Dit gebeurt bijvoorbeeld bij de ingang van universiteitsgebouwen, maar ook tijdens evenementen of protesten.

Het controleren van identiteitsbewijzen en studentenpassen kan bijdragen aan het gevoel van studenten dat zij in de gaten worden gehouden. Hierdoor kan het een *chilling effect* hebben op het uitoefenen van grondrechten, zoals het demonstratierecht en de vrijheid van vergadering. Hiernaast is het voor studenten niet altijd duidelijk wat het doel is van de controle, wat de universiteit doet met de informatie die zij op de identiteitsbewijzen en studentenpassen zien, en of zij bijvoorbeeld namen opschrijven van mensen die naar bepaalde soort bijeenkomsten komen. In dit hoofdstuk wordt nader ingegaan op de regels omtrent het controleren van identiteitsbewijzen en studentenpassen.

Eerst over de controle van identiteitsbewijzen. Voor personen boven de 14 jaar oud geldt in Nederland een wettelijke identificatieplicht.⁸⁷ Volgens deze plicht zijn echter alleen politieagenten en ambtenaren van bijzondere opsporingsdiensten bevoegd om naar een officieel identiteitsbewijs te vragen.⁸⁸ Bovendien mag de politie alleen een identificatiebewijs vragen als hier een goede reden voor is, waaronder verstaan wordt 'als de politie redelijkerwijs uw identiteit nodig heeft om haar taak uit te voeren'.⁸⁹

Hiernaast mogen toezichthouders⁹⁰, conducteurs en financiële instellingen onder sommige omstandigheden identificatie vragen.⁹¹ Ook is het voor sommige diensten, zoals het verkopen van alcohol, bij een 18+ film of bij het ophalen van een pakket, toegestaan om identificatie te vragen.⁹²

Particuliere beveiligers mogen ook bezoekers van hun pand om identificatie vragen.⁹³ De verhouding tussen een universiteit en een student is echter anders dan die tussen bijvoorbeeld een kledingwinkel en een klant. In het eerste geval heeft de student in beginsel het recht om het universiteitsgebouw te betreden van de universiteit waaraan het collegegeld is betaald. Normaal gesproken zou een particuliere beveiligers een bezoeker de toegang kunnen weigeren omdat als de bezoeker geen identificatie wil laten zien. Dit lijkt op de universiteit echter moeilijker: de student heeft recht om op de universiteit te zijn en het onderwijs te volgen. Zoals hieronder zal blijken, zou in het geval van universiteiten moeten kunnen worden volstaan met het vragen van een studentenpas in plaats van een officieel identiteitsbewijs. Ook de studentenpas zou echter alleen gevraagd

⁸⁷ Artikel 2 Wet op de identificatieplicht.

⁸⁸ Artikel 2 Wet op de identificatieplicht.

⁸⁹ <https://www.rijksoverheid.nl/onderwerpen/identificatieplicht/vraag-en-antwoord/wie-mag-vragen-naar-mijn-identiteitsbewijs-en-wanneer>. Voorbeelden die door de Rijksoverheid aangehaald worden zijn: 'een auto rijdt 's nachts rond op een industrieterrein; na een schietpartij is het belangrijk voor het onderzoek om de identiteit van (mogelijke) getuigen vast te stellen; hangjongeren veroorzaken overlast in de openbare ruimte; (...) bij onrust of dreigend geweld in uitgaansgebieden en op openbare manifestaties' (<https://www.rijksoverheid.nl/onderwerpen/identificatieplicht/vraag-en-antwoord/wie-mag-vragen-naar-mijn-identiteitsbewijs-en-wanneer>).

⁹⁰ Toezichthouders zijn 'ambtenaren die toezicht moeten houden op de naleving van bepaalde wetten', zoals toezichthouders van bouw- en woningtoezicht en inspecteurs van de Nederlandse Arbeidsinspectie.

⁹¹ <https://www.rijksoverheid.nl/onderwerpen/identificatieplicht/vraag-en-antwoord/wie-mag-vragen-naar-mijn-identiteitsbewijs-en-wanneer>

⁹² <https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/paspoort-en-identiteitskaart/identiteitsbewijs-bij-koop-huur-of-verkoop>

⁹³ <https://www.rijksoverheid.nl/onderwerpen/identificatieplicht/vraag-en-antwoord/wie-mag-vragen-naar-mijn-identiteitsbewijs-en-wanneer>

moeten worden wanneer dit een duidelijk doel dient en het noodzakelijk is om een studentenpas te vragen om dit doel te bereiken. Dit wordt hieronder nader toegelicht.

In hoofdstuk 5.1 over het controleren van tassen wordt toegelicht hoe een controlebeleid dat niet inzichtelijk is sneller kan leiden tot discriminatie. Als de universiteit besluit om niet alle studenten te controleren, zou zij helder moeten formuleren en communiceren op basis van welke criteria wel om een studentenpas gevraagd wordt om te controleren of de betreffende persoon een student aan de universiteit is.

De AP besteedt ook expliciet aandacht aan wanneer het vragen van een identiteitsbewijs nodig is in het onderwijs. De AP noemt drie situaties: bij inschrijving, bij eindexamens en bij toetsen of tentamens.⁹⁴ In de eerste situatie, bij inschrijving aan een universiteit, is de universiteit wettelijk verplicht om de identiteit van de student vast te stellen. Hierbij is het niet toegestaan aan de onderwijsinstelling om een foto of kopie te maken van het identiteitsbewijs.⁹⁵

Over identificatie tijdens toetsen of tentamens legt de AP uit dat de universiteit kan vragen je te legitimeren tijdens een tentamen, waarbij de examiner of surveillant je kan vragen om je studentkaart of identiteitsbewijs.⁹⁶ Het doel hiervan is om fraude te voorkomen. De AP waarschuwt ook hier dat onderwijsinstelling geen foto of kopie van je identiteitsbewijs mogen maken.⁹⁷

In het licht van de covid-maatregelen, toen studenten vaak thuis tentamens moesten maken waarbij soms videosurveillance (proctoring) werd ingezet, legt de AP uit dat het in zo'n geval onmogelijk is om je studentpas of identiteitsbewijs te laten zien zonder dat hier een kopie (video-opname) van gemaakt wordt. De AP legt uit:

“Daarom mag je school of universiteit nooit vragen om je hele identiteitsbewijs te laten zien, zonder dat er gegevens zijn afgeschermd.

Je school of universiteit moet kiezen voor een manier van identificeren die zo min inbreuk maakt op de privacy van studenten. Het tonen van een studentkaart maakt bijvoorbeeld minder inbreuk dan het tonen van een identiteitsbewijs, omdat op een studentkaart minder (gevoelige) gegevens staan dan op een identiteitsbewijs.”⁹⁸

De AP legt verder uit dat wanneer er ‘echt geen andere mogelijkheid [is] om je te identificeren dan je identiteitsbewijs te laten zien’ bijvoorbeeld omdat je je studentenpas kwijt bent, dat je ‘universiteit je alleen [mag] vragen om een deels afgeschermd identiteitsbewijs te tonen’ waarbij je BSN niet zichtbaar is.⁹⁹ Als laatste merkt de AP op:

“De school of universiteit moet vooraf een duidelijke instructie geven aan alle studenten hoe zij zich kunnen identificeren. En als het tonen van een identiteitsbewijs noodzakelijk is, welke gegevens studenten dan mogen afschermen.”¹⁰⁰

⁹⁴ <https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/paspoort-en-identiteitskaart/identiteitsbewijs-in-het-onderwijs>

⁹⁵ <https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/paspoort-en-identiteitskaart/identiteitsbewijs-in-het-onderwijs>

⁹⁶ <https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/paspoort-en-identiteitskaart/identiteitsbewijs-in-het-onderwijs>

⁹⁷ <https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/paspoort-en-identiteitskaart/identiteitsbewijs-in-het-onderwijs>

⁹⁸ <https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/paspoort-en-identiteitskaart/identiteitsbewijs-in-het-onderwijs>

⁹⁹ <https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/paspoort-en-identiteitskaart/identiteitsbewijs-in-het-onderwijs>

¹⁰⁰ <https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/paspoort-en-identiteitskaart/identiteitsbewijs-in-het-onderwijs>

Het is dus aan de onderwijsinstelling om studenten te informeren hierover, en om aan te geven dat het Burgerservicenummer (“BSN”) moet worden afgeschermd.¹⁰¹

Universiteiten zouden dus voorzichtig moeten omspringen met het vragen van een officieel identificatiebewijs aan studenten. Dit zou alleen moeten gebeuren als het noodzakelijk is en wanneer niet met een minder ingrijpend middel kan worden volstaan. In vrijwel iedere situatie, buiten inschrijving en toetsing, zou de universiteit moeten kunnen volstaan met het vragen van een studentenpas, waardoor het vragen van een officieel identiteitsbewijs vrijwel nooit gerechtvaardigd lijkt.

Dit betekent echter niet dat universiteiten je altijd zouden moeten kunnen vragen om je te identificeren met je studentenpas. Zoals eerder toegelicht kan van het vragen om een identificatiebewijs, ook in de vorm van een studentenpas, een *chilling effect* op de uitoefening van verschillende grondrechten uitgaan. Het VN-Mensenrechtencomité legt bijvoorbeeld uit dat mensen het recht hebben om anoniem te demonstreren en moeten zij pas om identificatie gevraagd worden op het moment dat er bijvoorbeeld een redelijke verdenking van strafbaar handelen is.¹⁰² De mogelijkheid van een *chilling effect* werd bij de uitbreiding van de Wet op de identificatieplicht ook opgemerkt door de Nederlandse Vereniging voor Rechtspraak:

“De wetenschap dat van burgers op ruimere schaal legitimatie kan worden verlangd, zou hen ervan kunnen weerhouden aanwezig te zijn bij bepaalde evenementen of op bepaalde plaatsen, zodat de vrijheid van vergadering, van demonstratie of van meningsuiting in het gedrang kan komen”¹⁰³

Hier staat tegenover dat het onder sommige omstandigheden begrijpelijk kan zijn dat universiteiten willen controleren of iemand daadwerkelijk een student is aan die universiteit, zodat deze persoon ook echt het recht heeft om op de universiteit aanwezig te zijn. Om een *chilling effect* te voorkomen zouden universiteiten dit middel echter alleen in moeten zetten wanneer dit een duidelijk doel dient en het noodzakelijk is om een studentenpas te vragen om dit doel te dienen. Universiteiten zouden kunnen overwegen om studenten hierbij hun naam af te laten dekken zodat alleen de foto zichtbaar is. Dit zou voldoende kunnen zijn om te controleren of een student daadwerkelijk aan de universiteit studeert.

Universiteiten zouden in ieder geval geen lijsten moeten bijhouden van studenten die bij bepaalde bijeenkomsten aanwezig zijn of foto’s maken van identiteitsbewijzen en studentenpassen. Het lijkt zeer moeilijk om de noodzaak van zulke acties aan te tonen, en hierbij hebben ze een groot *chilling effect* op verschillende grondrechten van studenten. Hieronder wordt nader ingegaan op het fotograferen van identiteitsbewijzen.

4.2 Het fotograferen van een identiteitsbewijs of studentenpas

PILP heeft ook vragen gekregen over het fotograferen van identiteitsbewijzen en studentenpassen door beveiligingsmedewerkers van universiteiten. Studenten geven aan dat dit bijvoorbeeld gebeurt bij politieke bijeenkomsten en/of vergaderingen van bepaalde (politiek actieve) clubs en organisaties op de universiteit. Een foto van een identiteitsbewijs geldt als een kopie van een identiteitsbewijs en het maken hiervan is aan (strikte) regels onderworpen.

Er zijn maar weinig organisaties die bevoegd zijn om een volledige kopie van een identiteitsbewijs te vragen. Het gaat dan over, onder andere, overheidsinstanties, banken en verzekeraars. Werkgevers zijn vaak ook verplicht om een kopie van het identiteitsbewijs van hun werknemers te hebben.¹⁰⁴ Een volledige kopie (waaronder een foto) van een identiteitsbewijs mag alleen als dit in de wet bepaald is.¹⁰⁵ Universiteiten hebben niet de wettelijke

¹⁰¹ Autoriteit Persoonsgegevens 2020, p. 20-21.

¹⁰² VN-Mensenrechtencomité, ‘General comment No. 37(2020) on the right of peaceful assembly (article 21)’, 17 september 2020, CCPR/C/GC/37, para. 60.

¹⁰³ Kamerstukken II 2003-04, 29218, nr. 3, p. 4.

¹⁰⁴ <https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/vraag-en-antwoord/ben-ik-verplicht-om-een-kopie-van-mijn-identiteitsbewijs-te-geven-aan-een-bedrijf>

¹⁰⁵ <https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/paspoort-en-identiteitskaart/voor-organisaties-regels-voor-vaststellen-identiteit>

bevoegdheid om een foto te maken van het identiteitsbewijs van een student, zonder afscherming van bijvoorbeeld de pasfoto en het BSN.

Voor andere bedrijven geldt dat zij bijvoorbeeld wel een kopie mogen maken van het identificatiebewijs, maar dat bepaalde informatie, zoals de pasfoto en het BSN daarbij afgeschermd moet zijn. Het gaat hier dan bijvoorbeeld over telecombedrijven en autoverkopers.¹⁰⁶ Het maken van een gedeeltelijke kopie van een identiteitsbewijs mag alsnog alleen 'als het echt niet anders kan', eerst moet gekeken worden 'of er een minder ingrijpende manier mogelijk is'.¹⁰⁷

Weer andere organisaties zijn verplicht om bepaalde gegevens van het identiteitsbewijs over te nemen, zoals scholen bij inschrijving en zorgverleners. Het is echter niet nodig om hiervoor een kopie van het identiteitsbewijs te maken. Het is in zulke gevallen voldoende om op te schrijven om wat voor soort identificatiebewijs het gaat (bijvoorbeeld een paspoort) en wat het nummer hiervan is. Weer andere organisaties, denk aan hotels of een camping, mogen alleen noteren welk soort legitimatiebewijs is getoond.¹⁰⁸

Uit het bovenstaande en de vorige sectie blijkt dat het vrijwel zeker is dat universiteiten nooit een foto of kopie mogen maken van het officiële identiteitsdocument van studenten. Daar is geen rechtvaardiging of noodzaak voor. Mocht een student zich schuldig maken aan strafbare feiten, dan kan de universiteit de politie inschakelen. De politie heeft dan de bevoegdheid om officiële identificatie van de student te vragen.

Wat betreft het fotograferen van studentenpassen, zijn hier minder duidelijke regels voor. Dit is echter ook een zware ingreep in de privacy van studenten. Bovendien heeft het, zoals hierboven toegelicht, een *chilling effect* op de uitoefening van andere grondrechten. Universiteiten zouden, ook onder de AVG, moeten aantonen op basis van welke grondslag zij deze foto's maken, welk gerechtvaardigd doel dit dient, waarom het noodzakelijk is om een foto van de studentenpas te maken en hoe lang deze foto's bewaard worden.

5. Observatie studenten

Naast het identificeren van studenten, zien een aantal van de maatregelen van universiteiten ook op het observeren van studenten. Zoals hierboven toegelicht, zijn er geen of weinig specifieke regels gericht op universiteiten die zien op de privacy van studenten, en wat de universiteit binnen dit kader mag doen. Ook in dit hoofdstuk zullen dus meer algemene regels op het gebied van privacy worden toegepast op de situaties op universiteiten. Ook zijn verschillende regels die gelden voor werkgevers ten aanzien van hun werknemers relevant.

5.1 Het doorzoeken van tassen

PILP heeft van enkele studenten vernomen dat beveiligingsmedewerkers van universiteiten de tassen van studenten zouden controleren, ook terwijl de student dit niet wist (bijvoorbeeld terwijl iemand naar het toilet gaat).¹⁰⁹ Het doorzoeken van een tas is een vergaand controlemiddel welke een zware inbreuk kan maken op de

¹⁰⁶ Zij mogen een (gedeeltelijke) kopie maken om identiteitsfraude tegen te gaan en bijvoorbeeld 'achteraf te kunnen bewijzen wie het telefoonabonnement heeft afgesloten'. In het geval van het huren van een auto, mag er bijvoorbeeld alleen een (gedeeltelijke) kopie van het identiteitsbewijs gemaakt worden voor zover dit noodzakelijk is voor het doel: bij een autoverhuurder kan dit doel liggen in het aangifte doen als de auto wordt gestolen door de huurder. Zodra de auto teruggebracht wordt, moet de kopie wel vernietigd of teruggegeven worden.

<https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/vraag-en-antwoord/ben-ik-verplicht-om-een-kopie-van-mijn-identiteitsbewijs-te-geven-aan-een-bedrijf>

¹⁰⁷ <https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/paspoort-en-identiteitskaart/voor-organisaties-regels-voor-vaststellen-identiteit>

¹⁰⁸ <https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/vraag-en-antwoord/ben-ik-verplicht-om-een-kopie-van-mijn-identiteitsbewijs-te-geven-aan-een-bedrijf>

¹⁰⁹ Zie bijvoorbeeld <https://sleutelstad.nl/2024/08/27/universiteit-leiden-onder-vuur-om-schending-privacy-studenten/>.

Ook kondigde de UvA aan het begin van het huidige academische jaar (2024-2025) aan toegangscontroles met QR-codes in

privacy van studenten. Omdat er geen specifieke regels voor universiteiten zijn op dit punt, worden de regels voor controle door werkgevers van personeel hier besproken alsmede de inbreuk die tassencontroles op verschillende grondrechten kunnen hebben.

In de AVG en de UAVG zijn regels opgenomen voor de controle door werkgevers van hun werknemers. Hier gelden een aantal algemene vereisten voor waar de controle in ieder geval aan moet voldoen. Dit zijn (i) gerechtvaardigd belang (ii) noodzaak (iii) informatieplicht (iv) instemming OR (v) DPIA (vi) voorafgaande raadpleging AP.¹¹⁰ Deze voorwaarden zijn in het algemene hoofdstuk over de AVG nader uitgewerkt.

Als de controle geheim is, gelden nog extra voorwaarden. Organisaties moeten hierbij voldoen aan alle normale criteria voor controle, maar ook aan extra regels. Voordat een werkgever heimelijke controle mag inzetten, moet er een redelijke verdenking bestaan dat de medewerkers iets strafbaars doen.¹¹¹ Bovendien moet de controle noodzakelijk en subsidiair zijn: het moet met andere middelen niet gelukt zijn om een einde te maken aan de strafbare feiten, denk aan diefstal of fraude, en de werkgever moet niet anders kunnen dan geheime controle in te zetten.¹¹²

Bovendien is het niet toegestaan om continu geheim te controleren. Deze controle mag slechts incidenteel zijn en mag alleen plaatsvinden in een vooraf bepaalde periode. Verder moet de organisatie de werknemers achteraf altijd informeren dat er geheime controle heeft plaatsgevonden, ook als er niks uit de controle komt. De eerste keer dat een organisatie heimelijke controle inzet, moet er een DPIA plaatsvinden met advies van de FG. Als de geheime controle uitgevoerd wordt door een particulier recherchebureau, moeten zij een DPIA uitvoeren. Ook hier geldt dat bij een hoog privacyrisico, voorafgaande raadpleging van de AP moet plaatsvinden.¹¹³

Het doorzoeken van tassen kan ook raken aan het privéleven van de student in algemene zin, zoals beschermd door artikel 8 EVRM. Zo kan je tas veel persoonlijke informatie bevatten, zoals welke medicijnen je neemt, een foto van je geliefde of moeder of andere persoonlijke spullen. Het EHRM overwoog eerder in het kader van een 'stop and search area' dat tassencontrole door de autoriteiten een inbreuk op artikel 8 kan opleveren:

"Irrespective of whether in any particular case correspondence or diaries or other private documents are discovered and read or other intimate items are revealed in the search, the Court considers that the use of the coercive powers conferred by the legislation to require an individual to submit to a detailed search of his person, his clothing and his personal belongings amounts to a clear interference with the right to respect for private life. Although the search is undertaken in a public place, this does not mean that Article 8 is inapplicable. Indeed, in the Court's view, the public nature of the search may, in certain cases, compound the seriousness of the interference because of an element of humiliation and embarrassment. Items such as bags, wallets, notebooks and diaries may, moreover, contain personal information which the owner may feel uncomfortable about having exposed to the view of his companions or the wider public."¹¹⁴

te gaan zetten bij bepaalde evenementen, waar ook jassen en tassen niet meegenomen mochten worden, de UvA stelde dat er 'geen directe aanleiding' was voor deze maatregelen (<https://www.nrc.nl/nieuws/2024/08/30/tassencontroles-en-gr-codes-bij-uva-en-vu-vanwege-gevoelens-van-onveiligheid-onder-joodse-studenten-en-medewerkers->).

¹¹⁰ <https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/voorwaarden-voor-controle-werknemers>

¹¹¹ <https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/voorwaarden-voor-heimelijke-controle-werknemers#:~:text=Normaal%20gesproken%20is%20heimelijke%20controle,ingrijpend%20kan%20zijn%20voor%20werk-emers>

¹¹² <https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/voorwaarden-voor-heimelijke-controle-werknemers#:~:text=Normaal%20gesproken%20is%20heimelijke%20controle,ingrijpend%20kan%20zijn%20voor%20werk-emers>

¹¹³ <https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/voorwaarden-voor-heimelijke-controle-werknemers#:~:text=Normaal%20gesproken%20is%20heimelijke%20controle,ingrijpend%20kan%20zijn%20voor%20werk-emers>

¹¹⁴ EHRM 12 januari 2010, app. no. 4158/05 (*Gillan en Quinton vs. het Vereniging Koninkrijk*), r.o. 63.

Belangrijk hierbij voor het EHRM is dat het individu overal gestopt kan worden, zonder kennisgeving of keuze om zich te onderwerpen aan een doorzoeking.¹¹⁵

Bovendien leent een tassencontrolebeleid dat niet inzichtelijk is en niet gecommuniceerd wordt, zich sneller voor discriminatie. In januari 2024 oordeelde het College voor de Rechten van de Mens nog dat een supermarkt zich schuldig had gemaakt een directe discriminatie op grond van ras bij een tassencontrole.¹¹⁶ De supermarkt had een '100% controle beleid' en een bord in de winkel hangen waarop stond dat alle tassen gecontroleerd worden. Bij de kassa vroeg de caissière om in de tas van een jongen te kijken. Uit camerabeelden van de supermarkt bleek dat de klanten voor en achter de jongen niet gecontroleerd werden. De jongen had een donkere huidskleur en de andere klanten een lichte.¹¹⁷ Het College overweegt:

"Het feit dat de tas van de zoon van verzoekster wel is gecontroleerd, terwijl bij enkele klanten geen tassencontrole is uitgevoerd, betekent naar het oordeel van het College dat de tassencontrole niet consistent is en daardoor niet transparant en controleerbaar is. Het College overweegt dat het vaste oordelenlijn is dat procedures inzichtelijk, controleerbaar en systematisch moeten worden uitgevoerd. Dit is noodzakelijk omdat anders het risico bestaat dat bewust of onbewust verboden onderscheid wordt gemaakt en bovendien geen controle of toetsing van de procedure meer mogelijk is. Als een procedure weinig inzichtelijk is en/of niet op objectieve wijze wordt uitgevoerd, kan dit bijdragen aan het vermoeden dat onderscheid is gemaakt

(...)

Het College oordeelt derhalve dat verweerster jegens verzoekster verboden onderscheid op grond van ras heeft gemaakt door haar beleid voor een 100% controle niet consistent, transparant en controleerbaar uit te voeren en bij het afrekenen van boodschappen te vragen de tas van haar zoon te openen ter controle."¹¹⁸

Universiteiten zouden de mogelijkheid tot tassencontrole minstens op moeten nemen in de huisregels en duidelijk moeten communiceren naar studenten waar, wanneer en waarom zij onderwerp kunnen zijn van zulke controles. De conclusie dat universiteiten altijd tassencontroles zouden mogen uitvoeren als zij voldoen aan deze twee vereisten, zou echter te vergaand zijn. In het licht van privacywetgeving en de grondrechten van studenten, moet de controle namelijk ook noodzakelijk, proportioneel en subsidiair zijn.

Momenteel lijkt het er niet op dat universiteiten voldoen aan de bovengeschetste vereisten voor (heimelijke) controle van tassen voor studenten. Mede omdat tassencontrole een grove inbreuk kan maken op het privéleven van studenten, zullen universiteiten ook niet snel voldoen aan deze vereisten. Gezien het gebrek aan communicatie over de ingezette veiligheidsmaatregelen en de rechtvaardiging hiervoor, is dit echter lastig te controleren. Volgens de AVG is het de verantwoordelijkheid van de universiteiten om aan te tonen dat zij voldoen aan de vereisten van de AVG. Op het moment van schrijven voldoen universiteiten niet aan deze verantwoordingsplicht.

5.2 Het maken van foto's en video's van studenten tijdens bijeenkomsten

Studenten geven ook aan dat beveiligingsmedewerkers foto's en video's van hen maken tijdens bijeenkomsten en protesten. Hierbij wordt niet gecommuniceerd waarom er beeldmateriaal gemaakt wordt en wat hiermee gebeurt. Studenten geven aan het gevoel te hebben in de gaten gehouden te worden en minder vrijelijk gebruik te (kunnen) maken van hun rechten, zoals de vrijheid van vergadering en vereniging.

Verskillende overwegingen spelen een rol bij de vraag of de universiteit dit mag doen. Zo mag je foto's en video's maken waar andere mensen herkenbaar op staan als het beeldmateriaal voor persoonlijk gebruik is.¹¹⁹ Hier is in onderhavig geval duidelijk geen sprake van. Verder kan een onderwijsinstelling of werkgever

¹¹⁵ Ibid, r.o. 64.

¹¹⁶ College voor de Rechten van de Mens 30 januari 2024, oordeelnummer 2024-10.

¹¹⁷ Ibid, overwegingen 3.1&4.7.

¹¹⁸ College voor de Rechten van de Mens 30 januari 2024, oordeelnummer 2024-10, overwegingen 4.8&4.12.

¹¹⁹ <https://www.autoriteitpersoonsgegevens.nl/themas/internet-slimme-apparaten/beeldmateriaal>

beeldmateriaal van leerlingen of medewerkers maken voor bijvoorbeeld promotiemateriaal. Hier heeft de onderwijsinstelling toestemming van de studenten en medewerkers voor nodig.¹²⁰ Dit kan bijvoorbeeld bij de inschrijving van de student geregeld worden, maar bij een wijziging van de verwerking moet opnieuw toestemming worden gevraagd.¹²¹ Bovendien kunnen werknemers en studenten deze toestemming intrekken, en zouden hier geen negatieve gevolgen aan verbonden moeten worden.¹²²

Het beeldmateriaal wat verzameld wordt tijdens deze bijeenkomsten, lijkt echter niet bedoeld te zijn voor publicatie op de website of voor promotiemateriaal. Het lijkt dan ook onaannemelijk dat de universiteit toestemming heeft voor deze verzameling en verwerking van persoonsgegevens. Het is onduidelijk voor welk doel het beeldmateriaal wel wordt gemaakt. Als het bijvoorbeeld gedaan wordt om te registreren wie aanwezig is bij bepaalde evenementen of wie meedoet aan een protest, komen de mensenrechten van studenten in het gedrang. Zoals hierboven toegelicht, hebben mensen het recht om anoniem te demonstreren en vergaderen. Alleen als er sprake is van strafbare feiten of de dreiging hiervan door specifieke personen, zouden zij geïdentificeerd mogen worden. Ook komt de vrijheid van vergadering onder druk te staan als universiteiten bijhouden wie naar welke bijeenkomsten gaat. Studenten zullen zich niet vrij voelen om aan te sluiten bij bepaalde bijeenkomsten als zij weten dat de universiteit ze in de gaten houdt. Deze praktijk kan dus een groot *chilling effect* hebben op de uitoefening van verschillende mensenrechten door studenten.

Hiernaast kan beargumenteerd worden dat het hier gaat om bijzondere persoonsgegevens, namelijk persoonsgegevens waaruit iemands politieke opvattingen blijken. Uit het beeldmateriaal van specifieke bijeenkomsten kan namelijk blijken welke politieke opvattingen de student op de foto heeft. Het verwerken van persoonsgegevens waaruit politieke opvattingen blijken, is verboden onder de AVG.¹²³ Hier zijn bepaalde uitzonderingen op mogelijk, zoals wanneer de betrokkene uitdrukkelijke toestemming heeft gegeven.¹²⁴ Zoals hierboven toegelicht, lijkt hiervan geen sprake te zijn op de universiteiten.

Een andere uitzonderingsgrond is als er sprake is van een zwaarwegend algemeen belang.¹²⁵ Dit is verder uitgewerkt in de UAVG voor drie situaties: (i) de verwerking is noodzakelijk om aan een volkenrechtelijke verplichting te voldoen (ii) de gegevens worden verwerkt door de AP of een ombudsman waarbij de verwerking noodzakelijk is voor het uitvoeren van hun wettelijk opgedragen taken (iii) de verwerking is noodzakelijk in aanvulling op de verwerking van persoonsgegevens van strafrechtelijke aard voor de doeleinden waarvoor deze gegevens worden verwerkt.¹²⁶ Ook deze uitzonderingsgrond lijkt dus niet op te gaan.

Een onderdeel van de zorgen van studenten hierover is dat ook onduidelijk is hoe lang de universiteit het beeldmateriaal bewaart. In het licht van opnames van lessen en tentamens tijdens de coronapandemie, overwoog de AP:

“De AP wijst er op dat beeldmateriaal enkel zo lang mag worden bewaard als noodzakelijk is voor het doeleinde waarvoor de persoonsgegevens worden verwerkt. Indien online proctoring bijvoorbeeld alleen wordt ingezet voor het doel om fraude te voorkomen en de identiteit van de student te controleren, terwijl niet is gebleken dat de student tijdens het tentamen heeft gefraudeerd, dan dienen de beelden na de identiteitscontrole te worden verwijderd.”¹²⁷

¹²⁰ <https://www.autoriteitpersoonsgegevens.nl/themas/internet-slimme-apparaten/beeldmateriaal/beeldmateriaal-in-het-onderwijs> & <https://www.autoriteitpersoonsgegevens.nl/themas/internet-slimme-apparaten/beeldmateriaal/beeldmateriaal-op-de-werkplek>

¹²¹ <https://www.autoriteitpersoonsgegevens.nl/themas/internet-slimme-apparaten/beeldmateriaal/beeldmateriaal-in-het-onderwijs>

¹²² <https://www.autoriteitpersoonsgegevens.nl/themas/internet-slimme-apparaten/beeldmateriaal/beeldmateriaal-op-de-werkplek>

¹²³ Artikel 9 lid 1 AVG.

¹²⁴ Artikel 9 lid 2 sub a AVG.

¹²⁵ Artikel 9 lid 2 sub g AVG.

¹²⁶ Artikel 23 UAVG.

¹²⁷ Autoriteit Persoonsgegevens 2020, p. 18.

Wanneer besloten wordt dat het bewaren van bepaald beeldmateriaal wel noodzakelijk is, dan dient het materiaal opgeslagen te worden in een beveiligde omgeving waar alleen geautoriseerd personeel van de universiteit toegang toe heeft.¹²⁸

Concluderend is onduidelijk op welke grond de universiteit meent foto's en video's van studenten te kunnen maken tijdens bepaalde bijeenkomsten, voor welk doel zij dit doet en wat er met het beeldmateriaal gebeurt. Hierbij is het belangrijk om de wettelijke taken van universiteiten in gedachten te houden: het verzorgen van wetenschappelijk onderwijs, het verrichten van wetenschappelijk onderzoek en het overdragen van kennis.¹²⁹ Zij zijn niet wettelijk belast met het verzorgen van de algemene veiligheid of het opsporen van strafbare feiten.

5.3 Het inzetten van beveiliging in burger

Het inzetten van beveiliging in burger door universiteiten kan verschillende regels raken. Ten eerste de regels over beveiliging in burger op zichzelf: wanneer moet een beveiliging herkenbaar zijn en wanneer niet. En ten tweede regels over heimelijke controle in het algemeen: wanneer mag er bijvoorbeeld heimelijk cameratoezicht ingezet worden.

De Wet particuliere beveiligingsorganisaties en recherchebureaus stelt regels voor het uniform van particuliere beveiligers. Artikel 9 van deze wet bepaald dat de beveiligingsorganisatie zorg draagt dat de beveiligers tijdens hun werkzaamheden 'een door Onze Minister goedgekeurd uniform dragen'. Voor bepaalde werkzaamheden kan de minister van Justitie en Veiligheid ontheffing verlenen van deze verplichting, 'indien dit gelet op de aard van de werkzaamheden gewenst is en zich daartegen geen zwaarwegende belangen verzetten'.¹³⁰ Zulke ontheffing kan bijvoorbeeld verleend worden voor persoonsbeveiliging, winkelsurveillance en de beveiliging van een luchtvaartterrein.¹³¹

Aan ongeüniformeerde beveiliging zijn extra eisen verbonden. Zo moeten beveiligers zonder uniform een extra diploma gehaald hebben.¹³² Verder is toegelicht dat de ontheffing alleen verleend wordt indien 'het gestelde doel van de beveiliging niet in redelijkheid op andere wijze (derhalve geüniformeerd) kan worden bereikt'.¹³³ Zoals gezegd, wordt geen ontheffing verleend 'indien zwaarwegende belangen zich tegen de verlening van de ontheffing verzetten', zoals dat de vereiste diploma's ontbreken.¹³⁴

Specifiek op het inzetten van beveiliging zonder uniform om winkeldiefstal te verminderen, wordt het volgende overwogen. Voor een ontheffing

“wordt bezien welke preventieve maatregelen de winkelier al heeft getroffen om winkeldiefstal tegen te gaan. Bij het verlenen van de ontheffing voor dit doel geldt als voorwaarde dat er sprake dient te zijn van een evenwichtige verhouding tussen de inzet van geüniformeerde en ongeüniformeerde beveiligers. Bijzondere aandacht bij de instructie van het personeel in deze gevallen dient te worden gegeven aan de handelwijze bij het aanhouden van personen. De ongeüniformeerde beveiliging dient zich tegenover de aangehouden persoon onverwijld als particulier beveiliging te legitimeren.”¹³⁵

Ook is de ontheffing gebonden aan een termijn.¹³⁶

Een eerste vraag is dus of universiteiten, of een specifieke universiteit, de benodigde ontheffing heeft voor het inzetten van beveiliging in burger. Een tweede vraag is of de universiteiten voldoen aan de strikte criteria voor

¹²⁸ Autoriteit Persoonsgegevens 2020, p. 18.

¹²⁹ Artikel 1.3 WHW.

¹³⁰ Artikel 9 lid 2 Wet particuliere beveiligingsorganisaties en recherchebureaus en artikel 12 Regeling particuliere beveiligingsorganisaties en recherchebureaus.

¹³¹ <https://ondernemersplein.kvk.nl/uniformdraagplicht-voor-particuliere-beveiligingsorganisaties/>

¹³² Artikel 9 lid 1 Regeling particuliere beveiligingsorganisaties en recherchebureaus.

¹³³ Artikel 6.2 Beleidsregels particuliere beveiligingsorganisaties en recherchebureaus 2019.

¹³⁴ Artikel 6.2 Beleidsregels particuliere beveiligingsorganisaties en recherchebureaus 2019.

¹³⁵ Ibid.

¹³⁶ Ibid.

heimelijke controle. Hierboven is besproken dat voor geheime controle van werknemers, bijvoorbeeld door het inzetten van camera's, er sprake moet zijn van een redelijke verdenking van strafbaar gedrag door werknemers. Ook moet de controle noodzakelijk en subsidiair zijn: geheime controle moet alleen ingezet worden als er geen andere manier is om te zorgen dat de strafbare feiten stoppen. Hiernaast mag er niet continu geheim gecontroleerd worden en moeten werkgevers na de controle de werknemers informeren over de controle. Bovendien moet er een DPIA plaatsvinden en overleg met de FG en mogelijk voorafgaande raadpleging van de AP.

Het is onduidelijk in hoeverre de universiteiten voldoen aan de bovenstaande eisen op privacygebied, bijvoorbeeld of er een DPIA is uitgevoerd en hoe veel en vaak er beveiliging in burger wordt ingezet. Ook is onduidelijk of de universiteiten de ontheffing hebben voor het inzetten van beveiliging in burger.

Hiernaast is de vraag opgeworpen of universiteiten wel de regels op het gebied van medezeggenschap hebben gevolgd.¹³⁷ Zo zou in ieder geval in één specifiek geval de universiteitsraad niet om advies gevraagd zijn, terwijl dit op grond van artikel 9.33a WHW wel nodig zou zijn geweest.¹³⁸ Zelfs als de universiteit dus de benodigde ontheffing heeft en hard kan maken dat deze geheime controle noodzakelijk is, waar sterk aan getwijfeld kan worden, is het dus de vraag of de maatregelen op de correcte manier tot stand zijn gekomen.

5.4 Het lezen van e-mails van studenten en werknemers

PILP heeft ook vragen ontvangen over het meelezen van e-mails van studenten en medewerkers door universiteiten. Het lezen van e-mails van werknemers door werkgevers is onderhavig aan verschillende regels. Binnen het kader van de universiteit is reden om aan te nemen dat vergelijkbare regels gelden voor het lezen van e-mails van studenten. Het is zelfs te beargumenteren dat er strengere regels gelden voor de universiteit wanneer zij de e-mails van studenten controleren, omdat de universiteit er bijvoorbeeld geen belang bij heeft om te checken of een student de studentenmail ook privé gebruikt. Dit zou wel relevant kunnen zijn wanneer het aankomt op de e-mails van werknemers: Het kan voor een werkgever van belang zijn om te weten of de werknemer de professionele e-mail voor privé zaken gebruikt, en of de werknemer tijdens werktijd veel bezig is met privé zaken. Zulke belangen gaan voor het meelezen met e-mails van studenten niet op.

Het controleren van werknemers door werkgevers in het algemeen moet voldoen aan verschillende voorwaarden, zoals we hierboven hebben gezien. Zo moet de controle voldoen aan privacywetgeving, de controle moet noodzakelijk zijn en het belang van de organisatie moet zwaarder wegen dan de inbreuk op de privacy van de werknemer.¹³⁹ Onder het controleren van werknemers valt het meelezen van e-mails, maar ook het inzetten van cameratoezicht. Voor alle vormen van dit soort controle, geldt dat deze moet voldoen aan de algemene privacywetgeving neergelegd in de AVG en de UAVG.

In deze privacywetgeving staat dat de organisatie een gerechtvaardigd belang bij de controle moet hebben die zwaarder weegt dan de rechten en belangen van de werknemer, zoals privacyrechten. Het is aan de organisatie om dit belang te beargumenteren. Verder moet de controle noodzakelijk zijn en moet er geen andere, minder ingrijpende manier zijn om het doel van de werkgever te bereiken. Ook is het belangrijk dat de organisatie de werknemers van te voren informeert over wat wel en niet mag, waar dus werkmail bijvoorbeeld wel en niet voor ingezet mag worden. Hierbij moeten de werknemers geïnformeerd worden over op welke manier er gecontroleerd wordt en welke gegevens hierbij bekeken worden. Deze informatie kan bijvoorbeeld gecommuniceerd worden via interne richtlijnen, gedragsregels en/of protocollen.¹⁴⁰

¹³⁷ <https://www.mareonline.nl/nieuws/universiteitsraad-stop-per-direct-met-beveiligers-in-burger/>

¹³⁸ Ibid.

¹³⁹ <https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/voorwaarden-voor-controle-werknemers>

¹⁴⁰ <https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/voorwaarden-voor-controle-werknemers>

Verder moeten werkgevers bij het controleren van e-mails rekening houden met het recht op vertrouwelijke communicatie. Het is dus niet toegestaan om privémails te lezen. Bovendien is dit een soort geval waarvoor de universiteit toestemming moet vragen aan de OR. Zonder instemming mag de werkgever niet controleren.¹⁴¹

Als het gaat om grootschalige verwerking van persoonsgegevens of om stelselmatige monitoring om de activiteiten van werknemers te controleren (zoals het gebruik van e-mail of via cameratoezicht) dan is de werkgever verplicht om eerst een DPIA uit te voeren. De werkgever moet dus een inschatting maken van de privacyrisico's van de controle en het systeem dat hiervoor gebruikt wordt. Ook moet de organisatie advies vragen aan de FG.¹⁴² Als uit de DPIA komt dat de controle een hoog privacyrisico oplevert, dan moeten er maatregelen genomen worden om dit te beperken. Als dit moeilijk is, dan is het aan de organisatie om voorafgaande raadpleging bij de AP te doen.¹⁴³

Specifiek op het punt van controle van communicatiemiddelen, moet de organisatie vooraf laten weten wat de regels zijn omtrent het gebruik van de e-mail en dat mensen mogelijk gecontroleerd kunnen worden. Als je hier geen richtlijn over hebt als organisatie, kan je bijvoorbeeld privégebruik van e-mail niet volledig verbieden omdat je ook recht hebt op een mate van privacy tijdens je werk.¹⁴⁴ Het monitoren kan via een steekproef plaatsvinden. Voorafgaand aan de controle moet bepaald worden voor welk doel dit noodzakelijk is. Van dit doel hangt dan weer af hoe omvangrijk de controle mag zijn en welke controlemiddelen ingezet mogen worden. Bij vermoedens van misbruik van de e-mail door specifieke werknemers, kan onder bepaalde voorwaarden een kortdurende gerichte controle naar diens e-mail plaatsvinden.¹⁴⁵ Aangezien dit een heimelijke controle is, moet deze controle voldoen aan de hierboven genoemde voorwaarden voor geheime controle naast de normale vereisten voor controle.¹⁴⁶ Zoals hierboven toegelicht, zouden studenten nog meer beschermd moeten zijn tegen het meelesen van e-mails dan werknemers, omdat zij geen arbeidscontractuele verplichtingen hebben ten aanzien van de universiteit.

Wederom is onduidelijk in hoeverre universiteiten voldoen aan deze criteria omdat er een gebrek aan communicatie is over welke maatregelen ingezet worden en wanneer en waarom deze ingezet worden. Het is echter aan de universiteit om aan te tonen dat zij voldoet aan de voorwaarden uit de AVG. Aan deze verplichting voldoet de universiteit op dit moment niet.

6. Conclusie

De (nieuwe) veiligheidsmaatregelen die universiteiten inzetten, kunnen zeer ingrijpend zijn voor studenten. Zo kunnen deze maatregelen een grote impact hebben op hoe veilig en vrij studenten zich op de universiteit voelen. Ook kunnen zij een *chilling effect* hebben op grondrechten zoals de vrijheid van meningsuiting, vergadering en vereniging. Veel van de maatregelen raken ook aan de privacyrechten van studenten, en het recht op privéleven in het algemeen.

Zo lijkt er geen rechtvaardiging te bestaan om een officieel identiteitsbewijs van studenten te vragen buiten situaties als inschrijving en tentamens. Ook het vragen van een studentenpas kan een *chilling effect* hebben op de grondrechten van studenten, en zou alleen ingezet moeten worden als dit nodig is om een duidelijk doel te dienen. Verder heeft de universiteit niet het recht om een foto te maken van een officieel identiteitsbewijs en ziet PILP ook geen rechtvaardiging voor het fotograferen van de studentenpassen van studenten.

¹⁴¹ <https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/voorwaarden-voor-controle-werknemers>

¹⁴² <https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/voorwaarden-voor-controle-werknemers>

¹⁴³ <https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/voorwaarden-voor-controle-werknemers>

¹⁴⁴ <https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/controle-van-communicatiemiddelen>

¹⁴⁵ <https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/controle-van-communicatiemiddelen>

¹⁴⁶ Zo moet er sprake zijn van een redelijke verdenking, noodzakelijkheid en subsidiariteit.

Op het gebied van observatie en controle is de universiteit onderworpen aan strenge regels, zeker als het gaat om geheime controle. Maatregelen zoals het controleren van tassen, het maken van foto's en video's van studenten, het inzetten van beveiliging in burger en het lezen van e-mails van studenten, kunnen allemaal inbreuk maken op de privacyrechten van studenten, hun recht op privéleven en/of een *chilling effect* hebben op de vrijheid van vergadering, vereniging en meningsuiting. Binnen dit kader zouden deze maatregelen alleen ingezet moeten worden als zij noodzakelijk, proportioneel en subsidiair zijn.

Hier komt bij dat van een aantal van de maatregelen onduidelijk is of zij voldoen aan andere wettelijke vereisten en of zij dus überhaupt ingezet mogen worden. Zo is niet duidelijk of universiteiten de benodigde ontheffing hebben om beveiliging in burger in te zetten en of er wel een grondslag bestaat op basis waarvan universiteiten de e-mails van studenten zouden mogen lezen.

Bovendien geldt voor alle genoemde maatregelen dat het de vraag is of zij tot stand zijn gekomen met de vereiste instemming of het vereiste advies van medezeggenschapsorganen op de universiteit. Zeker als het gaat om ingrijpende maatregelen, is de kans groot dat de universiteit dergelijke medezeggenschap nodig heeft voordat ze kan overgaan tot deze maatregelen.

Een terugkerend probleem bij de beoordeling van de maatregelen is het gebrek aan communicatie van de universiteiten over welke maatregelen zij inzetten, wanneer en op welke manier zij dit doen en voor welk doel. Al deze omstandigheden zijn relevant voor een oordeel of een maatregel voldoet aan de vereisten onder de AVG, en of deze noodzakelijk, proportioneel en subsidiair is. Onder de AVG ligt de verantwoordelijkheid voor het aantonen dat aan deze vereisten wordt voldaan, bij de universiteiten zelf. Op zijn minst kan dus geconcludeerd worden dat verschillende universiteiten niet voldoen aan deze verantwoordingsplicht. Het lijkt er echter sterk op dat de maatregelen ook niet voldoen aan andere wettelijke vereisten zoals gesteld door de AVG, de mensenrechtelijke kaders en verschillende Nederlandse wetten.