Security measures at universities

What is the university allowed to do?

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

Table of contents

NB This is a non-official translation of the Dutch version. No rights can be derived from this translation.

1. Introduction

Over the past year, several media reported on (new) far-reaching security measures deployed by several Dutch universities.[1] These include reports on the deployment of plainclothes security, (surreptitiously) checking bags, asking for and photographing IDs and student passes, and more. The PILP Foundation ("**PILP**") receives many questions from students and staff at various universities about whether these new security measures are in line with the law. This current report looks at these questions.

The university should be an open and safe place for everyone where discussion and exchange of ideas can take place freely. Moreover, the executive board, students and staff together constitute the university democracy, where a bond of trust and cooperation between these groups should exist. However, PILP is increasingly receiving reports that universities are imposing far-reaching security measures that may compromise various rights and freedoms, such as freedom of expression, assembly and association, and privacy rights.

In a study presented in January 2024 on the protection of personal data in education, the Dutch Data Protection Authority ("**DPA**") summarized the underlying issues regarding data processing at universities:

> "Educational institutions perform an important social task and are at the centre of society. After all, education is not only about imparting knowledge; educational institutions also have to deal with societal issues. They are expected to act more and more on these issues. Examples include the psychological well-being of pupils and students, safety, poverty, equality (of opportunity), polarization and reducing absenteeism.
>
> Despite these expectations and often well-meaning intentions, the question is whether there is an GDPR basis for educational institutions when they (further) process personal data for the aforementioned purposes, because the task of educational institutions on these points is often not (yet) clearly defined in law. Especially when it comes to very sensitive personal data, which educational institutions sometimes register and share with (public) organizations. The DPA sees that educational institutions do not always properly analyse whether this type of data processing is allowed and, if so, under what conditions. In addition, it is the legislator's role to provide new legislation if necessary. "[2] [2]

An DPA board member also described the importance of careful handling of student data and surveying this group:

> "From the sandbox to the college benches, education is the springboard that shapes your life. To discover who you are and make your dreams come true. And doing so while maintaining the standards that we value. Taking the privacy of pupils, students and teaching staff seriously is essential to this, so that education is actually the place where one can develop freely and protected. " [3]

Because there are only a few specific regulations that address what security measures universities are allowed to take, this report juxtaposes different (legal) frameworks to assess whether the current measures can legally stand. The first part of this report will discuss the more general frameworks of university democracy, human rights, privacy rules at universities in general and the internal competences of universities to employ security

---

[1] See, among others, https://www.nporadio1.nl/nieuws/binnenland/c71eb16b-79a3-40eb-9d6e 30f9c6bb7b91/studenten-concerned-about-security-measures-universities-observe-culture; https://nos.nl/artikel/2535105-security-measures-amsterdam-universities-at-opening-academic-year; https://www.ad.nl/binnenland/snap-het- grief-but safety-stands-foremost-university-utrecht-speaks-out-over-protests~a1f77851/

[2] Data Protection Authority Jan. 24, 2024, "Education Sector Assessment," p. 2. URL: https://www.autoriteitpersoonsgegevens.nl/documenten/sectorbeeld-onderwijs-2021-2023

[3] Data Protection Authority 2024, p. 4.

measures. On this last point,

both the representative advisory structures at universities and differences between private and public universities are taken into account.

The second part of this report looks at some specific measures that PILP has received many inquiries about. These measures see on identifying students by asking for and photographing their IDs and student passes. The measures also see on observing students by searching their bags, taking photos and videos of students, deploying plainclothes security, and reading student and employee emails.

PILP has also heard concerns about discrimination and ethnic profiling by security personnel at universities. For example, students of certain ethnicities would more often be subjects of said security measures, as well as members and visitors of organizations and events of certain political affinities. Universities should never engage in ethnic profiling or discriminatory practices. Further investigation of these practices is beyond the scope of the current report because their legality is not a subject of debate.

2. Executive Summary

There are several frameworks that apply to the security measures employed by different universities. A first framework is the university democracy. Even at the university, students must be able to exercise their fundamental rights, and the university, more than other private parties, must respect students' fundamental rights.

Security measures can have a *chilling effect* on various fundamental rights, such as freedom of expression, assembly and association. This is because students who are observed may not feel free to express their opinions or attend certain meetings. Privacy rights may also be compromised by the measures. Moreover, the measures may affect the right to private life in general.

Universities are bound by the General Data Protection Regulation ("**GDPR**"). Among other things, this means that universities' processing of personal data (including the collection thereof) must comply with several requirements. For example, any data processing must have a GDPR basis and any processing must serve a legitimate purpose. Furthermore, universities may not process more data than necessary for this purpose. Students have the right to inspection and right to objection under the GDPR.

Universities must comply with certain rules under the Higher Education and Scientific Research Act ("**HRA**") regarding participation in decision-making. Depending on the type of university, the university council or the works council have the right of consent or right to be consulted on certain issues. This structure can have an impact on the legality of the new measures: it is not always clear whether the measures were created through the proper route.

Furthermore, there are differences between public and special universities, specifically in the area of participation in decision-making. However, special universities are also bound by the GDPR and other relevant legislation.

Outside of registration or examinations, asking the university for official proof of identity does not seem justified or necessary and asking the student ID card should suffice. Frequent or unnecessary requests for proof of identity or student ID may have a *chilling* effect on the exercise of fundamental rights such as the right to demonstrate. Universities should therefore do so only when necessary. University photographing of an ID is almost never allowed. Photographing a student ID card is subject to the GDPR and is only allowed if there is a GDPR basis for this, it serves a legitimate purpose and no less intrusive means are possible.

The searching of bags is a drastic means of control that can have a major impact on students' right to privacy. Universities should only do this rarely and only if there are good reasons for this.

Secret checking of bags is subject to additional requirements and should only be done when there is reasonable suspicion of criminal activity.

Taking photos and videos of students during meetings falls under the collection of personal data and is therefore subject to the GDPR. The university needs a basis and legitimate purpose for this. It is unclear whether universities have this. Furthermore, this footage could qualify as special categories of personal data because students' political preferences could be derived from it. In that case, collecting this is prohibited and the university does not seem to have a ground that falls under any of the exceptions. In addition, this has a major *chilling effect* on students. It is also not clear what the university does with the footage and how long it keeps the footage. This practice does not seem to be in line with the GDPR.

The deployment of security in plain clothes is also subject to strict rules. First, security may only operate in plain clothes, and thus not in uniforms, if the university has an exemption to do so. It is not clear whether universities have this exemption. Second, it is questionable whether universities meet the strict requirements for covert surveillance.

The (covert) monitoring of students' and/or employees' emails must also meet strict requirements before it is allowed. It is not clear whether universities meet these requirements. In any case, continuous secret monitoring of email traffic is not allowed. In addition, it is questionable whether checking students' e- mails is allowed at all, since the reasons for checking that apply to employees (such as checking whether the work e
mail is not (too much) used for private purposes (during work)) do not apply to students. Also, students have no contractual obligations to the university .

In conclusion, there are many question marks and reservations about some (new) security measures of various universities. Especially in the area of privacy rights, it is highly questionable whether the university has a basis for the data processing it performs, and whether the data processing serves a legitimate purpose and is necessary. Also, in the area of transparency and information provision, universities do not seem to be meeting their obligations under the GDPR. For many of the measures, it is unclear why the universities perform them and in what, what they do with the information gathered, and whether the measures were properly established in the context of participation in decision-making. Students have the right to know what information is collected about them and why. They also have the right to be at the university, to participate in university democracy and to (anonymously) attend peaceful meetings and demonstrations. Some of the current policies at various universities have a *chilling effect* on various human rights and do not appear to be in line with privacy laws.

3. (Legal) framework

3.1 University democracy

Students pay tuition to be attending university, are often connected to the university for a longer period of time and have a legal right to participation in decision-making and to have a say in university policy. [4] Thus, they are part of the university democracy. The Association of Universities in the Netherlands explains that the idea behind, for example, the right to consent on the broad outlines of the university's budget is that "if students have to invest more for their studies, they should also have more influence on how public education funds are spent."[5] Moreover, representative advisory members are democratically elected, with every student having a vote.

[4] Which has been fought hard in the past to these rights, see, for example https://www.nationaalarchief.nl/beleven/onderwijs/bronnenbox/ontruiming-van-het-maagdenhuis-1969.

[5] Universities of the Netherlands, "How Participation in decision-making works at the University. https://www.universiteitenvannederland.nl/hoe-werkt-medezeggenschap-aan-de-universiteit (last visited: 28/11/2024).

This context colours how the university should deal with the (fundamental) rights of its students. Earlier, for example, PILP has argued that because of university democracy, the right to demonstrate extends further on university grounds than on other private grounds.[6] More than between other private parties, fundamental rights should have a horizontal effect between the university and the student. Educational institutions may, within the framework of the law, take security measures on their premises. In doing so, however, they must take into account the fundamental rights of their students and not restrict them unjustifiably or disproportionately.

3.2 Fundamental Rights

It is clear that some measures at universities, such as photographing identity cards and student passes, may affect students' privacy rights. However, these measures may also cause students to be restricted from exercising other fundamental rights, such as freedom of speech, assembly and association.

These fundamental rights and freedoms are enshrined in various human rights treaties, such as the European Convention on Human Rights ("**ECHR**"), the International Covenant on Civil and Political Rights ("**ICCPR**") and the Charter of Fundamental Rights of the European Union ("**EU Charter of Fundamental Rights**"). These fundamental rights are also enshrined in the Constitution.

(Covert) observation of students can have a *chilling* effect or deterrent effect on the exercise of these rights, particularly if identification and observation are used primarily and systematically at political events and meetings of political organizations active at the university. For example, the UN Human Rights Committee considers that surveillance can have a *chilling* effect on the right to demonstrate:

> "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 Netherlands ("**AIN**") reached a similar conclusion in a recent report:

> "Surveillance can discourage people from participating in demonstrations out of fear of being monitored. " [8]

And also Bart Schermer, professor of Law and Digital Technology at Leiden University concludes ''If you are watched all the time, you can no longer demonstrate freely.''[9] Universities need to be aware of these consequences and factor them into the assessments and judgments they make about the measures they want to deploy.

The DPA highlights a similar point in a study on the impact of online education and proctoring on students' privacy rights: not only should privacy rights be considered but also "risks touching on other (fundamental) rights and freedoms than just the right to protection of personal data should be taken into account."[10]

---

[6] PILP, "Analysis 'Directive on Protests Universities and Colleges' and the Right to Demonstrate. Available at: https://pilp.nu/juridische-analyse-demonstrerenop-universiteiten-en-hogescholen/

[7] UN Human Rights Committee, "General comment No. 37(2020) on the right of peaceful assembly (article 21)," September 17, 2020, CCPR/C/GC/37, para. 10.

[8] Amnesty International Netherlands, "In view of the police: Camera surveillance at peaceful protest in the Netherlands," October 2024, p. 3. URL: https://www.amnesty.org/en/documents/eur35/8469/2024/en/

[9] D. van Benthem et al, "Demonstration rights in ," Investico March 22, 2023, URL: https://www.platforminvestico.nl/onderzoeken/onderzoek-demonstratierecht-in-de-knel

[10] Data Protection Authority October 2020, "Investigation of online (video) calling and online proctoring in education," p. 3. URL: https://www.autoriteitpersoonsgegevens.nl/documenten/onderzoek-online-videobellen-en-online-proctoring-in-het education

Although the protection of human rights is primarily the task of governments, universities perform a legally mandated public task[11] and students are a part of the university democracy. For these reasons, there should be a horizontal effect of human rights such as the right to demonstrate between the university and the student.[12] Restrictions on these rights should therefore be necessary, proportionate, and subsidiary.[13]

In the area of privacy, all government agencies, companies and individuals in the Netherlands are bound by the GDPR.[14] In the GDPR, the criteria of necessity, proportionality and subsidiarity are specifically developed for restricting the right to privacy. Universities are also bound by the GDPR. What this means for universities is explained in more detail in the next section.

In addition to privacy rights in the sense of data processing and the GDPR, various measures may also affect students' rights to private life in general, within the meaning of Article 8 ECHR. The ECtHR has considered several measures used by governments to surveil citizens to be capable of violating their private lives.[15]

3.3 Privacy rules at universities

Many of the measures we discuss in this report touch on the privacy rights of students and employees. Thus, the general legal framework regarding the processing of personal data is relevant when assessing the legality of these measures. Overarching these rules are laid down in the GDPR. Universities, like other organizations in the Netherlands, must comply with the rules in the GDPR. These rules are further elaborated in the Dutch GDPR Implementation Act ("**GDPR Implementation Act**").

The GDPR establishes 6 basic principles for the processing of personal data (including collection)[16]: (i) lawfulness, fairness and transparency (ii) purpose limitation (iii) data minimisation (iv) accuracy (v) storage limitation and (vi) confidentiality and integrity.[17] In doing so, it is up to the processing entity to demonstrate compliance with these principles.[18] This is called the right to accountability and, in the context of this report, it lies with the universities.[19]

The DPA explains how organizations can comply with the right to accountability. For example, organizations are required to keep a record of processing activities[20], conduct a Data Protection Impact Assessment ("**DPIA**") 'on

---

[11] Namely, providing scientific education, conducting scientific research and transferring knowledge for the benefit of society (Article 1.3 HRA).

[12] The analysis on the right to demonstrate at educational institutions reaches the same conclusion (PILP, "Analysis 'Directive on Protests at Universities and Colleges' and the Right to Demonstrate. Available at: https://pilp.nu/juridische analysis-demonstrating-on-universities-and-high-schools/).

[13] As enshrined in human rights treaties such as the ECHR, ICCPR and the EU Charter on Fundamental Rights.

[14] These privacy rights are also enshrined in international human rights treaties.

[15] See, for example, on covert surveillance in , and the legal safeguards required in doing so ECHR 20 July 2021, app. nos. 58361/12, 25592/16, 27176/16 (*Zoltán Varga v. Slovakia*), para. 151. And on that surveillance of telephone calls may violate Article 8 ECHR, ECHR Jan. 12, 2023, app. no. 7286/16 (*Potoczká and Adamčo vs. Slovakia)*, r.o. 69. Similarly, subjecting a person to "stop and search" actions by the police may constitute a violation of private life (ECHR Jan. 14, 2021, app. no. 59648/13 (*Vig vs. Hungary*), para. 49).

[16] Processing personal data for personal use is not covered by the GDPR.

[17] Article 5(1) GDPR, summarized by the DPA (https://www.autoriteitpersoonsgegevens.nl/themas/basis-GDPR/GDPR general/de-GDPR-in-the short#:~:text=By%20the%20 General%20 Regulation%20data%20protection,they%20may%20get%20a%20fine%20).

[18] Article 5(2) in conjunction with Article 24 GDPR.

[19] And possibly with private security companies employed by universities.

[20] Article 30 GDPR.

data processing operations with a high privacy risk'[21]; maintain a data breach register; demonstrate 'that a data subject has actually consented to a data processing operation when you require consent for that processing'; substantiate why a Data Protection Officer ("**DPO**") has or has not been appointed[22] and prepare a privacy statement.[23]

The university is also required to enter into a processing agreement with a processor if data is processed by a third party on behalf of the university.[24] This could be important when using security guards from private companies. In addition, the DPO must be involved in all processes regarding the protection of personal data.[25]

For some organizations, it is also mandatory to have a privacy policy (in addition to the privacy statement, which is always mandatory). This depends on the nature, scope, context and purpose of the data processing.[26] This policy should show how the organization complies with the GDPR.[27]

The DPA signalled in 2024 that while most educational institutions do have a general privacy statement (as required) and privacy regulations, they "do not always include all of the educational institution's processing operations."[28] In doing so, the DPA notes that there is a desire from students "to have greater insight into who has access to their data, and to be able to influence this."[29]

Furthermore, a university must keep a record of processing activities.[30] This record contains certain information, such as the purposes for which personal data are processed. The record also contains a description of the (categories of) persons whose data are processed and categories of personal data that are processed.[31] The record also contains the date by which the data must be deleted and the recipients of the personal data, as well as how the personal data are protected.[32]

To comply with the first principle, lawfulness, the processing of personal data must be based on one of the legal bases in the GDPR. The bases are: (i) consent (ii) necessary for the performance of a contract (iii) necessary due to legal obligation (iv) necessary to protect vital interests (v) necessary to perform a task of public interest/public authority (vi)

---

[21] The university is required to conduct the DPIA prior to certain processing operations. This concerns, for example, "Large scale and/or systematic use of flexible camera surveillance. Here, the DPA emphasizes that conducting a DPIA is "a continuous process," requiring regular review and . In doing so, the DPA recommends that students, faculty and their representatives on various councils, be regularly asked for their views on data processing, "even if there is no legally binding right of advice or consent for these individuals or bodies" (Data Protection Authority 2020, p. 9).

[22] Article 37 GDPR.

[23] https://www.autoriteitpersoonsgegevens.nl/themas/basis-GDPR/GDPR-algemeen/verantwoordingsplicht

[24] Data Protection Authority 2020, p. 11.

[25] Data Protection Authority 2020, p. 15, Article 38 GDPR.

[26] https://www.autoriteitpersoonsgegevens.nl/themas/basis-GDPR/GDPR-algemeen/verantwoordingsplicht

[27] The DPA lists the following topics that could be : 'description of the categories of personal data you process; a description of the purposes for which you process personal data. And what the legal basis for this is'; how the principles of processing personal data are complied with, such as not processing more data than necessary; 'what privacy rights data subjects have and how they can exercise these rights'; what measures the organization has taken to secure the personal data and how long these are kept (https://www.autoriteitpersoonsgegevens.nl/themas/basis-GDPR/GDPR-algemeen/verantwoordingsplicht)

[28] Data Protection Authority 2024, p. 8.

[29] Data Protection Authority 2024, p. 8.

[30] Article 30 GDPR.

[31] https://www.autoriteitpersoonsgegevens.nl/themas/basis-GDPR/GDPR-algemeen/verantwoordingsplicht

[32] https://www.autoriteitpersoonsgegevens.nl/themas/basis-GDPR/GDPR-algemeen/verantwoordingsplicht

necessary to represent legitimate interests.[33] The DPA recommends that the legal basis for processing is stated in the privacy statement, privacy policy and in the record of processing activities.[34]

When it comes to processing special categories of personal data, extra strict rules apply. Special categories of personal data "are data that are so privacy-sensitive that it could have a big(ger) impact on a person if an organization were to process them."[35] This would include, for example, data "that can derive racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership."[36] The processing of these data is prohibited unless one of the grounds for exception is met.[37] Specifically with regard to the legal bases on which personal data can processed, the GDPR provides that public bodies, in the performance of their duties, are not entitled to invoke the legitimate interest basis[38]: 'Public educational institutions are therefore not entitled to invoke this legal basis in the performance of their duties.'[39]

Regarding the basis of consent, the DPA considers that a student:

> "must be able to freely consent to the processing of his or her personal data. The "free" element implies real choice and control for students. The relationship of authority between the educational institution and students may be problematic for invoking the basis of consent. After all, the question is whether students actually have the freedom to refuse consent vis-à-vis the educational institution when there are consequences prohibited. To be able to speak of free consent, the educational institution must in any case offer an alternative to the (intended) processing. If, when refusing consent, a student cannot attend their education or cannot participate in a test or examination, there is no free consent. Similarly, assuming that the student grants consent by participating in a digital lesson or an online proctoring exam is not lawful consent within the meaning of the GDPR. "[40]

Furthermore, the DPA emphasizes that the educational institution must be able to properly justify why a particular legal basis has been chosen and that the data processing is necessary to achieve the underlying purpose.[41]

---

[33] Article 6(1) GDPR. For further explanation of these bases, see https://www.autoriteitpersoonsgegevens.nl/themas/basis-GDPR/GDPR-algemeen/grondslagen-GDPR-uitgelegd

[34] https://www.autoriteitpersoonsgegevens.nl/themas/basis-GDPR/GDPR-algemeen/grondslagen-GDPR-uitgelegd

[35] https://www.autoriteitpersoonsgegevens.nl/themas/basis-GDPR/GDPR-algemeen/grondslagen-GDPR-uitgelegd#speciale-regels for-special-personal-data.

[36] Article 9(1) GDPR.

[37] The grounds for exception for processing special personal data, according to Article 9(2) GDPR, summarized by the DPA (https://www.autoriteitpersoonsgegevens.nl/themas/basis-GDPR/GDPR-algemeen/grondslagen-GDPR- explained#special-rules for-special-personal-data) are: (i) explicit consent (ii) necessary to carry out obligations or specific rights in the field of labor law, social security law and social protection law (iii) necessary to protect vital interests and the person in question is physically or legally incapable of giving his or her consent (iv) processing by a non-profit body that is politically, philosophically, religiously or active in a union (v) deliberately disclosed data by the person himself or herself (vi) necessary for a legal claim (vii) necessary for an important public interest (viii) necessary for preventive or medical purposes (ix) necessary for public health (x) necessary for archiving or research.

[38] Article 6(1) GDPR.

[39] Data Protection Authority 2020, p. 7.

[40] Data Protection Authority 2020, pp. 7-8.

[41] Data Protection Authority 2020, p. 8.

To comply with the first criterion, the data processing must be proper and transparent. This means it must not be "disadvantageous, discriminatory, unexpected or misleading" to the data subject.[42] It must also be transparent as to how and why the data is being processed.[43]

The second criterion, purpose limitation, sees that organizations must always have a legitimate purpose when processing personal data. The DPA explains:

> "That purpose must be specific and explicitly defined in advance. Thus, organizations should not start collecting personal data in advance because it might one day come in handy. "[44]

Also, the purpose of collecting the data must correspond to the purpose for which it is processed: "the organization may not suddenly start processing the data for a different purpose."[45]

Universities also must not process more data than necessary, as stipulated in the data minimisation requirement: "the processing of the data must be appropriate to the purpose" and "the organization [must] not process more data ... than is necessary to achieve that purpose."[46]Criterion four, accuracy, implies that organizations have a responsibility to ensure that inaccurate data is not processed, and that these are to be updated.[47] Criterion five, storage limitation, looks at the following: "Organizations must delete personal data once it is no longer needed for the original purpose for which it was collected."[48] Criterion six, confidentiality and integrity, implies that data processing operations must be properly secured.[49] Under the above criteria, organizations, and therefore universities, have certain obligations. For example, universities have a duty to inform those whose personal data they are processing.[50] The university must disclose to the data subject, amongst other, what personal data it processes, for what purposes, on what basis, and how long the data is kept.[51] There are also situations in which the university must provide more information. This depends, amongst others, on whether the use of your data is reasonably foreseeable, what consequences this use will have, and whether it involves sensitive data.[52] In doing so, the privacy statement that includes this information must be clear and not too long, complete and easy to find.[53]

In the context of information duties on educational institutions, the DPA previously considered:

> "In addition to the content of the information, attention should also be paid to the form in which the information is provided. Certainly (minor) students should not be expected to use complicated legal jargon understand or read lengthy privacy statements. Educational institutions should therefore provide the information in an accessible manner. "[54]

---

[42] https://www.autoriteitpersoonsgegevens.nl/themas/basis-GDPR/GDPR-algemeen/de-GDPR-in-het short#:~:text=By%20the%20General%20data%20protection%20regulation,%20they%20may%20be%20fined%20by%20the% 20fine%20.

[43] Ibid.

[44] Ibid.

[45] Ibid.

[46] Ibid.

[47] Ibid.

[48] Ibid.

[49] Ibid.

[50] Articles 12-14 GDPR. The organization does not always have to inform data subjects about the use of data, for example, if the data subject is already aware, or if there is disproportionate effort or a compelling interest. In the first case, the university must be certain that you are aware (https://www.autoriteitpersoonsgegevens.nl/themas/basis-GDPR/privacyrechten-GDPR/rech

[51] Article 13 GDPR.

[52] https://www.autoriteitpersoonsgegevens.nl/themas/basis-GDPR/privacyrechten-GDPR/recht-op-informatie

[53] https://www.autoriteitpersoonsgegevens.nl/themas/basis-GDPR/privacyrechten-GDPR/recht-op-informatie

[54] Data Protection Authority 2020, p. 21.

Students also have a right to inspection under the GDPR.[55] They have the right to hear from the university whether the university collects their personal data and to access the collected personal data.[56] In addition, students have the right to hear what the processing purposes from these collected data are, who receives the data and how long the data will be kept.[57]

Students also have a right to object under the GDPR: they have the right "to object to the processing of his or her personal data for reasons related to his/her particular situation."[58] Should a student object, the educational institution must stop data processing, "unless it can demonstrate that its overriding legitimate interests outweigh the interests or fundamental rights and freedoms of the data subject. This requires the educational institution to hold the interests of the student against those of the educational institution."[59] It is up to the educational institution to inform students of their right to object.[60]

3.4 Competences universities

3.4.1 Representative advisory and authority structure

The last framework to be discussed before turning to the legality of specific measures is the authority structure at universities. Indeed, the next section will show that there are conceivable situations in which certain measures can be deployed by the university, but it is highly questionable whether they have come about through the correct route. Indeed, for some far-reaching decisions, the university needs the consent of certain representative advisory councils, or they may issue an opinion. In determining what steps students may take to appeal to their university if they feel their rights are not (sufficiently) safeguarded, it is therefore also relevant whether the university has arrived at decisions about new security measures via the correct route.

Participation in decision-making at universities, and which bodies should be involved in taking (far-reaching) security measures, is regulated by the Higher Education and Scientific Research Act ("**HRA**").[61] In short, there are two variants. A university can have a University Council that includes both students and employees. In the second variant, the university has a Student Council and a Works Council and a joint council with delegates from these two councils.[62]

Special universities must adopt all rules from the HRA on participation in decision-making unless the nature of the university opposes this in the opinion of the Executive Board.[63] The Minister of Education, Culture and Science may also grant exemptions from certain legal requirements of the HRA at the request of the institution's management.[64]

---

[55] Article 15 GDPR.

[56] Article 15(1) GDPR.

[57] Article 15(1) GDPR.

[58] Data Protection Authority 2020, p. 24 on Article 21 GDPR. Students have this right only "if the basis of the processing is based on either the performance of a task carried out in the public interest or the exercise of official authority ... or legitimate interest" (Data Protection Authority 2020, p. 24 on Article 21(1) GDPR).

[59] Data Protection Authority 2020, p. 24.

[60] Data Protection Authority 2020, p. 24.

[61] https://www.universiteitenvannederland.nl/hoe-werkt-medezeggenschap-aan-de-universiteit

[62] W. Farmer March 4, 2020, "How does co-determination work at universities?", Association of Universities. URL: https://www.universiteitenvannederland.nl/files/publications/200224%20Hoe%20werkt%20de%20medezeggenschap%20-%20februari%202020.pdf. Sections 9.30 & 9.30a HRA.

[63] Article 9:51(2) HRA.

[64] https://lsvb.nl/dossiers/medezeggenschap/rechten-van-de-medezeggenschap/

Under the HRA, the council has the power to "make proposals and express points of view to the Executive Board on all matters relating to the university", to which the Executive Board must give a reasoned response.[65]The Executive Board also informs the university council of policies pursued and policy intentions on other organizational matters.[66] In addition, the Executive Board must timely provide the university council with all information that the council 'may reasonably and fairly need for the performance of its duties'.[67] Furthermore, the Executive Board requires the consent of the university council 'for each decision to be taken by the Executive Board concerning at least the adoption or amendment of' the institutional plan, the Students' Charter and the administrative and management regulations.[68]

In addition the university council also has advisory powers on decisions that relate to "matters of the continued existence and proper conduct of the university."[69]

If the university has a Works Council and the Executive Board has decided that the Works Councils Act ("**WOR**") applies[70], then the WOR lays down various rules regarding consent and advice. For example, consent must be sought from the Works Council if the university wishes to use personnel data or monitor employees[71]

Furthermore, the employer requires the consent of the Works Council for "any decision it proposes to take, amend or revoke (...) any regulation concerning the processing of, as well as the protection of, personal data of persons working in the enterprise.[72] Such consent is also required for regulations on "facilities aimed at or suitable for observing or monitoring the presence, behavior or performance of persons working in the enterprise."[73]

In addition, the Works Council also has the right to initiative to speak out on its own initiative about the use of personnel data.[74] The DPA cites as examples where this right can be used 'because of a security incident or questions or complaints from employees. Or something else where the Works Council believes the employer should take action.'[75] In a case, the Works Council can make an initiative proposal where the employer is required to make a decision.[76]

The Works Council also has the right to be consulted. The employer asks the Works Council for advice, among other things on "any proposed decision by it to (...) introduce or change a major technological facility."[77] This may include, for example, a new automation system or communication system.[78]

Specifically in the area of personnel tracking systems, the employer also needs the consent of the Works Council. Examples of personnel tracking systems are: 'a system that records attendance, time and access (

---

[65] Article 9.32(2) HRA.

[66] Article 9.32(5) HRA.

[67] Article 9.32(6) HRA.

[68] Article 9.33(1) HRA.

[69] Article 9.33a (1) (a) HRA.

[70] Within the meaning of Article 9.30(1)(a) WOR.

[71] https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/ondernemingsraad/de-rol-van-de-or-bij-privacy at-work

[72] Section 27 (1) introductory sentence and subsection k WOR.

[73] Article 27 (1) introductory phrase and (l) WOR.

[74] Section 23 (23) WOR.

[75] ttps://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/ondernemingsraad/de-rol-van-de-or-bij-privacy at-work

[76] https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/ondernemingsraad/de-rol-van-de-or-bij-privacy at-work

[77] Article 25 (1) introductory sentence and subsection k WOR.

[78] https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/ondernemingsraad/de-rol-van-de-or-bij-privacy at-work

software that records, for example, (...) email traffic (...) of employees; camera surveillance at the workplace.'[79] To set up such a system, the employer must seek the consent of the Works Council.[80] The DPA emphasizes here that the Works Council 'also has the right to consent in the case of a system that the employer is not (yet) using to track employees, but where this could be done.[81] 'Furthermore, it is important to critically review such a system, where the DPO can advise on whether the system is necessary, for example.[82]

As will be discussed further below, in some cases, questions have been raised as to whether the new security measures taken by universities have come about in accordance with this consent and advice framework.[83] One reason for this could be that the measures may have come about under (time) pressure. However, the DPA emphasizes, in a report on online education and proctoring during the corona pandemic, that temporary measures are often deployed on a permanent basis anyway, and therefore a close look should be taken at whether these measures meet all legal requirements:

> "Nevertheless, the DPA has also seen that educational institutions have not always given sufficient consideration to personal data protection issues when switching to remote education. Given the high urgency of this switchover and the major impact on education, this is understandable, but the DPA believes it is important for educational institutions to be transparent about this and still make every reasonable effort to take the appropriate safeguards on short-term, where this is necessary. After all, practice shows that "temporary" measures are also permanently deployed in the long term. It is therefore very important that when temporary solutions are implemented, even if they have to be implemented under time pressure, sufficient consideration is given to the protection of personal data. "[84] (underline added)

3.4.2 Differences between public and special universities

Most universities in the Netherlands are public universities. However, there are also "special" universities, founded by private individuals rather than the state. These are the Vrije Universiteit, Radboud University and Tilburg University.[85] These universities, as explained above, are obliged to adopt the participation in decision-making regulations from the HRA, unless the nature of the university precludes this.[86] It may therefore be the case that at special universities the representative authority councils have more or less rights on certain subjects. It is beyond the scope of this report to examine this for each university.

Furthermore, it could be argued that the private law status of special universities may have an impact on the extent to which students' human rights have horizontal effect and the extent to which university democracy is a relevant framework. It is also beyond the scope of this report to elaborate on this, mainly because there are simply no concrete rules or consensus on this. However, it would be going too far to argue that there is no university democracy at special universities: special universities must also regulate student and employee participation, with these two groups also having rights to be involved in these choices.

---

[79] https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/ondernemingsraad/de-or-en- personnel tracking systems

[80] Section 26 (1) (l) WOR.

[81] https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/ondernemingsraad/de-or-en- personnel tracking systems

[82] https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/ondernemingsraad/de-or-en- personnel tracking systems

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

[84] Data Protection Authority October 2020, "Investigation of online (video) calling and online proctoring in education," p. 3. URL: https://www.autoriteitpersoonsgegevens.nl/documenten/onderzoek-online-videobellen-en-online-proctoring-in-het education

[85] Appendix to the HRA, under b.

[86] Article 9.51(2) HRA.

It is also going too far to conclude that special universities do not have to respect the human rights of their students. At least on privacy rules, special universities are also bound by the GDPR. Many of the security measures discussed below touch on the GDPR. These sections apply equally to both types of universities. But other fundamental rights, such as the right to demonstrate, should also be respected by special universities.

4. Identification of students

4.1 Requesting proof of identity or student ID outside exams

A first measure deployed (recently) at universities is asking students to show proof of identity or student ID. This is done at the entrance to university buildings, for example, but also during events or protests.

Checking IDs and student passes can contribute to students' feeling that they are being watched. As a result, it can have a *chilling effect* on the exercise of fundamental rights, such as the right to demonstrate and freedom of assembly. In addition, it is not always clear to students what the purpose of monitoring is, what the university does with the information they see on IDs and student passes, and whether they write down names of people who come to certain types of meetings, for example. This chapter takes a closer look at the rules around checking IDs and student passes.

Firstly, the checking of identity documents. The Netherlands has a legal obligation to identify themselves for persons over 14 years old.[87] According to this obligation, however, only police officers and officials of special investigation services are authorized to ask for an official proof of identity.[88] Moreover, the police may only ask for proof of identity if there is a good reason for doing so, which means in practice "if the police reasonably need your identity to carry out their task."[89]

In addition, supervisors[90], conductors and financial institutions are allowed to ask for identification under some circumstances.[91] Identification is also allowed for some services, such as selling alcohol, at an 18+ movie or when picking up a package.[92]

Private security guards may also ask visitors to their premises for identification.[93] However, the relationship between a university and a student is different from that between, say, a clothing store and a customer. In the former case, the student has, in principle, the right to enter the university premises of the university to which tuition has been paid. Normally, a private security guard could refuse entry to a visitor because if the visitor does not want to show identification. However, this seems to be more difficult at the university: the student has a right to be at the university and receive the education. As will be shown below, in the case of universities, asking for a student pass instead of an official ID should suffice. However, even the student ID card should only be requested

---

[87] Article 2 Compulsory Identification Act.

[88] Article 2 Compulsory Identification Act.

[89] https://www.rijksoverheid.nl/onderwerpen/identificatieplicht/vraag-en-antwoord/wie-mag-vragen-naar-mijn ID-and-when . Examples cited by the central government are: 'a car drives around an industrial area at night; after a shooting, it is important for the investigation to establish the identity of (possible) witnesses; loitering youths cause a nuisance in public spaces; (...) in the event of unrest or imminent violence in nightlife areas and at public events" (https://www.rijksoverheid.nl/onderwerpen/identificatieplicht/vraag-en-answer/who may-ask-about-my-identity-proof-and-when).

[90] Supervisors are "officials whose job it is to supervise compliance with certain laws," such as building and housing supervision supervisors and inspectors from the Netherlands Labor Inspectorate.

[91] https://www.rijksoverheid.nl/onderwerpen/identificatieplicht/vraag-en-antwoord/wie-mag-vragen-naar-mijn ID-and-when

[92] https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/paspoort-en-identiteitskaart/identiteitsbewijs-bij-koop lease-or-sell

[93] https://www.rijksoverheid.nl/onderwerpen/identificatieplicht/vraag-en-antwoord/wie-mag-vragen-naar-mijn ID-and-when

when it serves a clear purpose and it is necessary to request a student pass to achieve this purpose. This is explained in more detail below.

Section 5.1 on checking bags explains how a checking policy that is not transparent can more quickly lead to discrimination. If the university decides not to check all students, it should clearly articulate and communicate on the basis of what criteria a student's pass will be asked to verify that the person is a student at the university.

The DPA also pays explicit attention to when asking for proof of identity is necessary in education. The DPA lists three situations: at registration, at final exams, and at tests or examinations.[94] In the first situation, at registration at a university, the university is required by law to establish the student's identity. Here the educational institution is not permitted to take a photograph or copy of the identity document.[95]

Regarding identification during tests or exams, the DPA explains that the university may ask you to identify yourself during an exam, in which case the examiner or invigilator may ask you for your student ID or proof of identity.[96] The purpose of this is to prevent fraud. Again, the DPA warns that educational institutions may not take a photo or copy of your ID.[97]

In light of the covid measures, when students often had to take exams at home that sometimes involved video surveillance (proctoring), the DPA explains that in such a case, it is impossible to show your student ID card or ID without a copy (video recording) being made of it. The DPA explains:

> "Therefore, your school or university should never ask to show your entire ID without data being shielded.
>
> Your school or university should choose a method of identification that is the least invasive of privacy as possible. For example, showing a student ID card infringes less than showing an ID card because a student ID card contains less (sensitive) data than an ID card. "[98]

The DPA further explains that when there is "really no other way [to] identify yourself than to show your ID," for example, because you have lost your student ID card, that your "university may only ask you to show a partially shielded ID" in which your BSN is not visible.[99] Finally, the DPA notes:

> "The school or university must provide clear instructions in advance to all students on how to identify themselves. And if showing proof of identity is necessary, what information students may shield. "[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 education

[96] https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/paspoort-en-identiteitskaart/identiteitsbewijs-in-het education

[97] https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/paspoort-en-identiteitskaart/identiteitsbewijs-in-het education

[98] https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/paspoort-en-identiteitskaart/identiteitsbewijs-in-het education

[99] https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/paspoort-en-identiteitskaart/identiteitsbewijs-in-het education

[100] https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/paspoort-en-identiteitskaart/identiteitsbewijs-in-het education

So it is up to the educational institution to inform students about this, and to indicate that the Citizen Service Number ("**BSN**") must be shielded.[101]

Universities should therefore exercise caution in requiring students to provide official identification. This should only be done when it is necessary and when a less intrusive means would not suffice. In almost every situation, outside of enrollment and testing, the university should be able to suffice with asking for a student ID, so asking for an official ID almost never seems justified.

However, this does not mean that universities should always be able to ask you to identify yourself with your student ID card. As explained earlier, asking for identification, even in the form of a student ID card, can have a *chilling* effect on the exercise of various fundamental rights. For example, the UN Human Rights Committee explains that people have the right to demonstrate anonymously and should only be asked for identification at the moment when there is, for example, a reasonable suspicion of criminal conduct.[102] The possibility of a *chilling effect* was also noted by the Dutch Association for the Judiciary when the Compulsory Identification Act was expanded:

> "The knowledge that legitimacy may be more widely required of citizens could discourage them from attending certain events or in certain places so that freedom of assembly, demonstration or expression may be compromised. "[103]

> On the other hand, under some circumstances it may be understandable that universities may want to verify that someone is actually a student at that university so that this person actually has the right to be present at the university. However, to avoid a *chilling effect*, universities should employ this tool only when it serves a clear purpose and it is necessary to request a student pass to serve this purpose. Universities might consider having students cover their names in the process so that only the photo is visible. This could be sufficient to verify that a student is actually studying at the university.

In any case, universities should not keep lists of students attending certain meetings or take pictures of IDs and student passes. It seems very difficult to prove the need for such actions, and in doing so, they have a great *chilling effect* on various fundamental rights of students. The following will have a closer look at photographing identity cards.

4.2 Photographing an ID or student ID card

PILP has also received questions regarding the photographing of identity cards and student passes by university security personnel. Students indicate that this happens, for example, at political rallies and/or meetings of certain (politically active) clubs and organizations at the university. A photo of an identity card counts as a copy of an identity card and taking pictures is therefore subject to (strict) rules.

Only a few organizations are authorized to request a full copy of an ID. These include, amongst others, government agencies, banks and insurance companies. Employers are also often required to have a copy of their employees' ID.[104] A full copy (including a photograph) of an ID is allowed only if decided by law.[105]

---

[101] Data Protection Authority 2020, pp. 20-21.

[102] UN Human Rights Committee, "General comment No. 37(2020) on the right of peaceful assembly (article 21)," September 17, 2020, CCPR/C/GC/37, para. 60.

[103] Parliamentary Papers (Kamerstukken) II 2003-04, 29218, no. 3, p. 4.

[104] https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/vraag-en-antwoord/ben-ik-verplicht-om-een-kopie-van my-identity-certificate-to-give-to-a-corporation

[105] https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/paspoort-en-identiteitskaart/voor-organisaties-regels pre-fix-identity

Universities do not have the legal authority to take a photograph of a student's ID without shielding such things as the passport photo and BSN.

For other companies, for example, they may make a copy of the identification document, but certain information, such as the passport photo and the BSN, must be protected.[106] Making a partial copy of an identity document is still only allowed "if there is no other option available", first there must be examined "whether there is a less invasive way possible."[107]

Yet other organizations are required to take certain information from the ID, such as schools upon enrollment and health care providers. However, in these circumstances it is not necessary to make a copy of the ID. In such cases, it is sufficient to write down what type of identification document is involved (for example, a passport) and what its number is. Yet other organizations, like hotels or a campground, may only note what type of identification has been shown.[108]

From the aforementioned, it is almost certain that universities should never take a photograph or copy of students' official identity documents. There is no justification or need for this. Should a student be guilty of criminal acts, the university may involve the police. The police then have the authority to request official identification from the student.

As for photographing student passes, the rules are less clear. However, this is also a heavy intrusion into student privacy. Moreover, as explained above, it has a *chilling* effect on the exercise of other fundamental rights. Universities, even under the GDPR, would have to demonstrate on what basis they take these photos, what legitimate purpose this serves, why it is necessary to take a photo of the student pass and how long these photos are kept.

5. Observation of students

In addition to identifying students, some of the measures taken by universities also see to the observation of students. As explained above, there are no or few specific rules regarding what universities are allowed to do when it comes to observation of their students. This chapter will therefore apply more general privacy rules to university situations. Various rules that apply to employers with respect to their employees are also relevant.

5.1 Bag searching

PILP has heard from some students that university security officers would check students' bags, even when the student was not aware of this (e.g. while someone is going to the restroom).[109] The searching of bags is a far going means of control, which can gravely infringe the privacy of students.

---

[106] They may make a (partial) copy in order to prevent identity fraud and, for example, "prove afterwards who took out the telephone subscription. In the case of renting a car, for example, they may only make a (partial) copy of the ID insofar as it is necessary for the : in the case of a car rental company, this purpose may lie in reporting if the car is stolen by the renter. Once the car is returned, however, the copy must be destroyed or returned. https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/vraag-en-antwoord/ben-ik-verplicht-om-een-kopie-van-mijn identity-giving-to-a-corporation

[107] https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/paspoort-en-identiteitskaart/voor-organisaties-regels pre-fix-identity

[108] https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/vraag-en-antwoord/ben-ik-verplicht-om-een-kopie-van my-identity-certificate-to-give-to-a-corporation

[109] See, for example, https://sleutelstad.nl/2024/08/27/universiteit-leiden-onder-vuur-om-schending-privacy-studenten/. Also, at the beginning of the current academic year (2024-2025), the UvA announced access controls with QR codes into start putting up coats and bags at certain events, where coats and bags were also not allowed to be taken, the UvA stated that there was "no immediate reason" for these measures (https://www.nrc.nl/nieuws/2024/08/30/tassencontroles-en-qr- codes-at-uva-and-vu-because-of-feelings-of-insecurity among-Jewish-students-and-employees).

Because there are no specific rules for universities on this issue, the rules for control by employers are discussed here as well as the potential infringement that bag checks can have on various fundamental rights.

The GDPR and the GDPR Implementation Act include rules for the monitoring of employees by their employers. There are a number of general requirements that the monitoring must meet in any case. These are (i) legitimate interest (ii) necessity (iii) information obligation (iv) consent of Works Council (v) DPIA (vi) prior consultation DPA.[110] These requirements are detailed in the general chapter on the GDPR.

If the controlling is covert, additional conditions apply. Organizations must meet all the normal criteria for monitoring, but also the additional rules. Before an employer may deploy covert monitoring, there must be a reasonable suspicion that the employees are doing something criminal.[111] In addition, the monitoring must be necessary and subsidiary: it must not have been possible to put an end to the criminal acts by other means, such as theft or fraud, and the employer must have no choice but to deploy covert monitoring.[112]

Moreover, continuous covert control is not permitted. Covert control may only be incidental and may only take place during a predetermined period. Furthermore, the organization must always inform employees afterwards that covert monitoring has taken place, even if nothing comes out of the monitoring. The first time an organization deploys covert monitoring, a DPIA must take place with advice from the DPO. If the covert monitoring is conducted by a private investigation agency, they must conduct a DPIA. Again, if there is a high privacy risk, prior consultation with the DPA must take place.[113]

Searching bags can also touch on a student's private life in a general sense, as protected by Article 8 ECHR. For example, your bag may contain a lot of personal information, such as what medication you take, a photo of your loved one or mother, or other personal items. The ECtHR previously considered in the context of a "stop and search area" that bag checks by authorities can violate Article 8:

> " 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]

---

[110] https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/voorwaarden-voor control-employees

[111] https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/voorwaarden-voor covert-control workers#:~:text=Normal%20spoken%20is%20secret%20control,profound%20can%20be%20for%20workers emers

[112] https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/voorwaarden-voor covert-controlworkers#:~:text=Normal%20spoken%20is%20secret%20control,profound%20can%20be%20for%20workers emers

[113] https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/voorwaarden-voor covert-control workers#:~:text=Normal%20spoken%20is%20secret%20control,profound%20can%20be%20for%20workers emers

[114] ECHR 12 January 2010, app. no. 4158/05 (*Gillan and Quinton v. the Association Kingdom*), para. 63.

Important here for the ECtHR is that the individual can be stopped anywhere, without notice or choice to submit to a search.[115]

Moreover, a bag check policy that is not transparent and not communicated lends itself more readily to discrimination. As recently as January 2024, the Institute for Human Rights ruled that a supermarket was guilty of direct racial discrimination in a bag check.[116] The supermarket had a "100% check policy" and a sign in the store stating that all bags are checked. At checkout, the cashier asked to look in a boy's bag. Camera footage from the supermarket showed that the customers in front of and behind the boy were not checked. The boy had a dark complexion and the other customers a light one.[117] The Board considered:

> "The fact that the bag of the applicant's son was checked, while at some customers no bag check was carried out, means, in the opinion of the Institute, that the bag check is not consistent and therefore not transparent and verifiable. The Institute considers that it is an established line of judgment that procedures must be transparent, verifiable and systematic. This is necessary because otherwise there is a risk that consciously or unconsciously prohibited distinctions will be made and furthermore no control or review of the procedure is possible anymore. If a procedure has little insight and/or is not carried out in an objective manner, this may contribute to the suspicion that discrimination has been made
>
> (...)
>
> Therefore, the Institute finds that the respondent made prohibited racial distinctions against the applicant, failing to implement its 100% verification policy in a consistent, transparent and verifiable manner and by asking to open her son's bag for verification when checking out groceries. "[118]

Universities should at least include the possibility of bag checks in house rules and clearly communicate to students where, when and why they may be the subject of such checks. However, concluding that universities should always be allowed to conduct bag checks if they meet these two requirements would be going too far. Indeed, in light of privacy laws and students' fundamental rights, checks must also be necessary, proportionate and subsidiary.

Currently, it does not appear that universities meet the requirements outlined above for (covert) bag checking for students. Partly because bag checking can grossly infringe on students' private lives, universities are not likely to comply with these requirements either. However, given the lack of communication about the security measures deployed and their justification, this is difficult to monitor. According to the GDPR, it is the responsibility of universities to demonstrate compliance with its requirements. At the time of writing, universities are not meeting this accountability requirement.

5.2 Taking photos and videos of students during meetings

Students also report that security personnel take photos and videos of them during rallies and protests. There is no communication as to why footage is taken and what happens to it. Students say they feel they are being watched and are less able to freely use their rights, such as freedom of assembly and association.

Several considerations play a role in whether the university is allowed to do this. For example, you may take photographs and videos in which other people are recognizable if the visual material is for personal use.[119] This is clearly not the case in this instance. Furthermore, an educational institution or employer may

---

[115] Ibid, r.o. 64.

[116] Institute for Human RIghts January 30, 2024, judgment number 2024-10.

[117] Ibid, recitals 3.1&4.7.

[118] Institute for Human RIghts January 30, 2024, judgment number 2024-10, recitals 4.8&4.12.

[119] https://www.autoriteitpersoonsgegevens.nl/themas/internet-slimme-apparaten/beeldmateriaal

take images of students or employees for promotional materials, for example. For this, the educational institution needs the consent of the students and employees.[120] This can be arranged, for example, when the student is enrolled, but consent must be requested again when the processing is changed.[121] Moreover, employees and students can revoke this consent, and there should be no negative consequences.[122]

However, the visual material collected during these meetings does not appear to be intended for publication on the website or for promotional material. Therefore, it seems implausible that the university has permission for this collection and processing of personal data. It is unclear for what purpose the footage is indeed being created. For example, if it is done to record who attends certain events or who participates in a protest, students' human rights are compromised. As explained above, people have the right to demonstrate and meet anonymously. Only if there are crimes or the threat of crimes by specific individuals should they be identified. Freedom of assembly also comes under pressure if universities keep track of who goes to which meetings. Students will not feel free to join certain meetings if they know the university is monitoring them. Thus, this practice can have a major *chilling* effect on students' exercise of various human rights.

In addition, it can be argued that these are special personal data, namely personal data that reveal a person's political views. Indeed, the footage of specific meetings may reveal the political views of the student in the photo. Processing personal data revealing political views is prohibited under the GDPR.[123] Certain exceptions to this are possible, such as when the data subject has given explicit consent.[124] As explained above, this does not appear to be the case at universities.

Another ground for exception is if there is a substantial public interest.[125] This is further elaborated in the GDPR Implementation Act for three situations: (i) the processing is necessary to comply with an obligation under international law (ii) the data are processed by the DPA or an ombudsman whereby the processing is necessary for the performance of their legally assigned tasks (iii) the processing is necessary in addition to the processing of personal data of a criminal nature for the purposes for which these data are processed.[126]Thus, this ground for exception also does not seem to apply.

Part of students' concerns about this is that it is also unclear how long the university retains the footage. In light of recordings of classes and exams during the corona pandemic, the DPA considered:

> "The DPA points out that footage should be kept only as long as necessary for the purpose for which the personal data are processed. For example, if online proctoring is only used for the purpose of preventing fraud and verifying the student's identity, when it is not proven that the student committed fraud during the examination, the images should be deleted after the identity check. "[127]

[120] https://www.autoriteitpersoonsgegevens.nl/themas/internet-slimme-apparaten/beeldmateriaal/beeldmateriaal-in-het education & https://www.autoriteitpersoonsgegevens.nl/themas/internet-slimme devices/imaging/imaging-in-the-workplace

[121] https://www.autoriteitpersoonsgegevens.nl/themas/internet-slimme-apparaten/beeldmateriaal/beeldmateriaal-in-

[123] Article 9(1) GDPR.

[124] Article 9(2)(a) GDPR.

[125] Article 9(2)(g) GDPR.

[126] Article 23 GDPR Implementation Act

[127] Data Protection Authority 2020, p. 18.

If it is decided that retention of certain footage does become necessary, the material should be stored in a secure environment to which only authorized university personnel have access.[128] In conclusion, it is unclear on what basis the university believes it can take photos and videos of students during certain meetings, for what purpose it does so, and what happens to the footage. Here it is important to keep in mind the legal duties of universities: providing academic education, conducting scientific research and transferring knowledge. [129]They are not legally charged with providing general security or investigating criminal offenses.

5.3 Deploying covert security

Universities' use of covert or plainclothes security can touch upon several rules. First, the rules about security in plainclothes per se: when must a security guard be recognizable and when can they be unrecognizable. And second, rules about covert surveillance in general: for example, when can covert camera surveillance be deployed.

The Act on Private Security Organizations and Detective Agencies sets rules for the uniform of private security guards. Article 9 of this Act states that the security organization shall ensure that security guards wear 'a uniform approved by Our Minister' during their work. For certain activities, the Minister of Justice and Security can grant exemption from this obligation, 'if this is desirable in view of the nature of the work and there are no significant interests against it'.[130] Such exemption can be granted, for example, for personal security, store surveillance and airport security.[131]

Non-uniformed security officers are subject to additional requirements. For example, non-uniformed security guards must have obtained an additional diploma.[132] It was further explained that the exemption will only be granted if "the stated goal of security cannot reasonably be achieved in any other way (i.e., uniformed)."[133] As stated, an exemption will not be granted "if a significant interest opposes the granting of the exemption," such as that the required diplomas are lacking.[134]

Specifically on the use of security without uniform to shoplifting, the following is considered. For an exemption

> "shall be considered what preventive measures the retailer has already taken to counter shoplifting. In granting the exemption for this purpose, the condition is that there must be a balanced ratio between the deployment of uniformed and non-uniformed security guards. Special attention in instructing personnel in these cases should be given to the course of action when apprehending persons. The non-uniformed security guard should immediately identify himself to the arrested person as a private security guard. "[135]
>
> The exemption is also subject to a time limit.[136]

So, a first question could be whether universities, or a specific university, has the necessary exemption to deploy covert security. A second question is whether universities comply to the strict criteria for

[128] Data Protection Authority 2020, p. 18.

[129] Article 1.3 HRA.

[130] Section 9 (2) Private Security Organizations and Detective Agencies Act and Section 12 Private Security Organizations and Detective Agencies Regulations.

[131] https://ondernemersplein.kvk.nl/uniformdraagplicht-voor-particuliere-beveiligingsorganisaties/

[132] Article 9 (1) Private Security Organizations and Detective Agencies Regulation.

[133] Section 6.2 Policy Rules Private Security Organizations and Detective Agencies 2019.

[134] Section 6.2 Policy Rules Private Security Organizations and Detective Agencies 2019.

[135] Ibid.

[136] Ibid.

covert surveillance. It was discussed above that for covert surveillance of employees, such as by deploying cameras, there must be reasonable suspicion of criminal conduct by employees. Also, the surveillance must be necessary and subsidiary: covert surveillance should only be deployed if there is no other way to ensure that the criminal acts stop. In addition, secret monitoring must not be used continuously and employers must inform employees about the monitoring after the monitoring. In addition, there must be a DPIA and consultation with the DPO and possibly prior consultation with the DPA.

It is unclear to what extent universities are complying with the above privacy requirements, such as whether a DPIA has been conducted and how much and how often civilian security is deployed. It is also unclear whether the universities have the exemption to deploy security in plain clothes.

Besides this, the question has been raised whether universities have followed the rules in the field of participation in decision-making.[137] For example, in at least one specific case, the University Council would not have been asked for advice, whereas it would have been required under section 9.33a HRA.[138] Thus, even if the university has the necessary exemption and can substantiate that this secret control is necessary, which can be strongly doubted, the question is whether the measures have been arrived at in the correct way.

5.4 Reading students´ and employees´ emails

PILP has also received questions about the reading of student and employee emails by universities. The reading of employee emails by employers is subject to different rules. Within the university framework, there is reason to believe that similar rules apply to reading student emails. It can even be argued that stricter rules apply to the university when checking student emails, because the university has no interest, for example, in checking whether a student uses the student email privately. This might be relevant when it comes to employee emails, though: It might be of interest to an employer to know whether the employee uses the professional email for private matters, and whether the employee is much engaged in private matters during working hours. Such interests do not apply to reading along with student emails.

The monitoring of employees by employers in general must meet several conditions, as we have seen above. For example, the monitoring must comply with privacy legislation, the monitoring must be necessary, and the interest of the organization must outweigh the invasion of the employee's privacy.[139] Monitoring employees includes reading emails, but also the use of camera surveillance. For all forms of this type of monitoring, it must comply with the general privacy legislation laid down in the GDPR and the GDPR Implementation Act.

These privacy laws state that the organization must have a legitimate interest in the audit that outweighs the employee's rights and interests, such as privacy rights. It is up to the organisation to argue this interest. Furthermore, the audit must be necessary and there must be no other, less intrusive way to achieve the employer's goal. It is also important that the organization informs the employees in advance about what is and is not allowed, i.e., what work email can and cannot be used for, for example. The employees must be informed about the way in which checks are carried out and which data are viewed. This information can be communicated, for example, via internal guidelines, rules of conduct and/or protocols.[140]

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

[139] https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/voorwaarden-voor control-employees

[140] https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/voorwaarden-

[138] Ibid.

Furthermore, employers must consider the right to confidential communication when checking emails. Thus, it is not allowed to read private emails. Moreover, this is a type of case for which the university must seek consent from the Works Council. Without consent, the employer may not check.[141]

When it concerns large-scale processing of personal data or systematic monitoring to control employees' activities (such as the use of e-mail or via camera surveillance), the employer is required to first conduct a DPIA. Thus, the employer must assess the privacy risks of the monitoring and the system used for this purpose. The organization must also seek advice from the DPO.[142] If the DPIA shows that the control poses a high privacy risk, then measures must be taken to reduce this. If this is difficult, then it is up to the organization to seek prior consultation with the DPA.[143]

Specifically on the issue of monitoring communication tools, the organization must let people know in advance what the rules are regarding the use of e-mail and that people can potentially be monitored. If you don't have a guideline on this as an organization, you can't completely prohibit private use of e-mail, for example, because you are also entitled to a degree of privacy while at work.[144] Monitoring can be done via sampling. Prior to monitoring, it must be determined for what purpose it is necessary. This purpose in turn depends on how extensive the monitoring may be and what means of monitoring may be used. In case of suspicion of misuse of the e-mail by specific employees, under certain conditions a short-term targeted check to their email may take place.[145] Since this is a covert monitoring, this monitoring must meet the above mentioned conditions for covert monitoring in addition to the normal requirements for monitoring.[146] As explained above, students should be even more protected from reading emails than employees, because they have no employment contractual obligations to the university.

Again, the extent to which universities meet these criteria is unclear because there is a lack of communication about what measures are deployed and when and why they are deployed. However, it is up to the university to demonstrate compliance with the requirements of the GDPR. The university does not currently meet this obligation.

6. Conclusion

The (new) security measures that universities deploy can be very invasive for students. For example, these measures can have a major impact on how safe and free students feel at the university. They can also have a *chilling effect* on fundamental rights such as freedom of speech, assembly and association. Many of the measures also affect students' privacy rights, and the right to private life in general.

For example, there seems to be no justification for requesting official ID from students outside of situations such as registration and exams. Similarly, asking for a student ID may have a *chilling* effect on students' fundamental rights, and should only be deployed when necessary to serve a clear purpose. Furthermore, the university does not have the right to take a photograph of an official ID, nor does PILP see any justification for photographing students' student passes.

[141] https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/voorwaarden-voor control-employees
[142] https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/voorwaarden-voor control-employees
[143] https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/voorwaarden-voor control-employees

[144] https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/controle-van communication tools

[145] https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers/controle-van communication tools

146 Thus, there must be reasonable suspicion, necessity and subsidiarity.

In the area of observation and monitoring, the university is subject to strict regulations, especially when it comes to covert surveillance. Measures such as checking bags, taking photos and videos of students, deploying plainclothes security and reading students' emails, can all infringe on students' privacy rights, their right to private life and/or have a *chilling effect* on freedom of assembly, association and expression. Within this framework, these measures should be used only if they are necessary, proportionate and subsidiary.

Added to this, it is unclear for some of the measures whether they meet other legal requirements and thus whether they may be deployed at all. For example, it is not clear whether universities have the necessary exemption to plainclothes security and whether a basis exists that would allow universities to read students' emails.

Moreover, for all the measures mentioned, it is questionable whether they have come about with the required consent or advice of representative authority bodies. Especially if the measures are far-reaching, it is likely that the university will require such participation before it can proceed with them.

A recurring problem in assessing the measures is the lack of communication from universities about what measures they deploy, when and how they do so, and for what purpose. All of these circumstances are relevant to an assessment of whether a measure meets the requirements under the GDPR, and whether it is necessary, proportionate and subsidiary. Under the GDPR, the responsibility for demonstrating that these requirements are met lies with the universities themselves. At the very least, therefore, it can be concluded that several universities are not meeting this accountability requirement. However, it strongly appears that the measures also fail to meet other legal requirements as set by the GDPR, human rights frameworks and various Dutch laws.