AUTORITEIT
PERSOONSGEGEVENS

Investigation report

Investigation of online voice and video calls and online proctoring in education

Report on definitive findings

Contents

1. Summary

The Dutch Data Protection Authority (DPA) observes that the education sector in the Netherlands had to make major changes during the COVID-19 crisis in order to ensure that, as far as possible, education could continue. Many educational institutions moved quickly to introduce applications for online voice and video calls, and sometimes also online proctoring. This has required a great deal of adaptability on the part of educational institutions and poses various challenges and risks.

In response to the large number of indications of potential issues and questions received by the DPA about personal data processing in remote online education, the DPA conducted an investigation in May, June and July 2020 on the use of online voice and video calling applications and online proctoring software in university education, higher professional education and secondary vocational education. The DPA notes that most of the educational institutions surveyed paid attention to the protection of personal data when facilitating remote education. Examples of best practice provided by the investigation are described in this report. Nevertheless, the DPA also notes that educational institutions have not always taken personal data protection issues sufficiently into account when switching to remote learning. This is understandable given the great urgency of this switch and its major impact on the educational sector, but the DPA considers it important for educational institutions to be transparent in this respect and, as a matter of priority, to make every reasonable effort to provide appropriate safeguards where necessary. Experience shows that 'temporary' measures frequently become permanent. For this reason, it is very important that the protection of personal data is given due consideration even when temporary solutions have to be implemented under time pressure. This is also consistent with the principle of privacy by design.

The DPA calls on all educational institutions to consider the following aspects when using online voice and video calls and/or online proctoring:

<u>Use of online applications</u>

- Before using online voice and video calls and online proctoring, determine and justify the purpose for which they will be used and the legal basis for this personal data processing operation.
- Perform a data protection impact assessment (DPIA) before using online voice and video calls and online proctoring; this is often mandatory. If possible, also involve the data subjects (the data subjects are the people to whom the data relates, i.e. in this case students and teachers). Periodically check whether the DPIA needs to be reviewed, for instance if COVID-19 measures are relaxed.
- When performing a DPIA, also take into account the risks that affect other (fundamental) rights and freedoms than solely the right to protection of personal data.
- Enter into a processing agreement with the supplier of the online application and ensure that the agreement meets the requirements of the General Data Protection Regulation (GDPR), at the very least. If dealing with suppliers outside the EEA, pay specific attention to ensuring that appropriate safeguards are in place.
- Before using online proctoring, always check whether there are alternative test formats that infringe students' privacy less. If online proctoring is used, the educational institution must record in writing why the use of online proctoring is necessary for certain tests and examinations.
- Involve the data protection officer (DPO) in good time if you intend to use online voice and video calls and online proctoring. Informing the DPO afterwards about how you have chosen to organise remote education is not sufficient.

Frameworks and guidelines for educational institutions

- Lay down institution-wide policies or guidelines on how to handle video footage in connection with online voice and video calls. At a minimum, the policy or guidelines should include agreements on:
  - showing students and teachers on screen and making recordings;
  - informing the data subjects about e.g. the purpose of the recording and the retention period;
  - if applicable: secure storage, the retention period and who is responsible for timely deletion of the recorded images.
- Lay down institution-wide policies or guidelines on remote testing. At a minimum, the policy or guidelines should include agreements on:
  - the cases in which online proctoring can be used;
  - the obligation to always first consider the options that least infringe students' personal data protection rights;
  - documenting the reasons for a decision by the educational institution to use online proctoring for a specific test or examination;
  - the means and methods used to process personal data of the data subjects;
  - how students provide proof of identity during digital tests. It is not permitted to have the student present their identity document with all the data visible.
  - obligatory human intervention in assessing whether a student might be committing fraud during a test or examination.
- Translate the policies/guidelines into clear and simple instructions.

Informing the data subjects

- Actively inform students about personal data processing prior to a digital lesson or test. Provide the information in an accessible and comprehensible way.
- Advise teachers and students to provide a neutral environment in which personal items are kept out of view while they are being filmed during a digital lesson or proctored test. Instruct students to turn off the camera and microphone if these functionalities are not necessary while attending a digital lesson.
- Inform students of their right to object to personal data processing. If a student objects to online proctoring and the educational institution cannot demonstrate that the interests of the institution outweigh those of the students, the educational institution must offer a suitable alternative that sufficiently alleviates the privacy concerns. This alternative should not be accompanied by any adverse consequences, such as a disproportionate delay to a person's studies.

2. Introduction

2.1 Background and context

The digital transformation of the education sector has accelerated rapidly in these extraordinary times. As a result of the measures taken in response to the COVID-19 crisis, many educational institutions quickly started looking for ways to continue providing education, as far as possible, by means of home learning. The increasing use of digital tools in education has proven its worth as a workable solution for organising remote education; millions of pupils and students have attended or are still attending lessons at home via an online voice and video calling application. In addition, some educational institutions use various applications for administering tests and examinations in which an invigilator or algorithm supervises the examination online, remotely, to prevent any student from committing fraud; this is known as online proctoring. Usually these applications use some form of camera surveillance. The emergence of online voice and video calling applications and online proctoring is leading to a shift in the traditional educational landscape. This shift brings with it new risks and challenges for educational institutions in terms of protecting the personal data of students and staff.

Parents, pupils, students and teachers have expressed concerns to the DPA regarding the data processing operations and associated risks associated with the large-scale use of (new) digital tools in education. The DPA shares these concerns.

That is why the DPA published instructions on 23 April 2020 for educational institutions that are using or intend to start using online voice and video calls and online proctoring. In response to complaints and indications of potential issues, the DPA also opened an investigation into the use of online voice and video calling applications and online proctoring in education. In this report, we share the results of this investigation.

2.2 Purpose and scope of the investigation

The DPA expects that the enforced introduction of remote teaching and testing will permanently change the practice of teaching in certain respects, even once COVID-19 measures have been relaxed in the future.

For this reason, the investigation serves multiple purposes. The primary aim of the DPA was to gain insight into personal data processing operations by educational institutions when using online voice and video calling applications and online proctoring. With this investigation, the DPA also wants to draw the attention of educational institutions and DPOs to the need to process personal data with all due care when using these digital tools. Finally, the DPA identified best practice and areas for improvement. The DPA aims to encourage the protection of students' and teachers' personal data in the way remote education is organised both now and in the future.

The DPA emphasises that the question of whether online voice and video calls or online proctoring can be used by an educational institution in a specific situation cannot be answered in general terms. This will have to be considered on a case-by-case basis, taking into account COVID-19 measures, among other factors. It is up to the educational institutions to determine whether the use of online proctoring and online voice and video calls is compliant with the requirements of the GDPR. The findings of the investigation can be used as a tool for reflection to assess current practice.

This investigation focuses on application of the GDPR to online voice and video calls and online proctoring. It does not consider the applicability of other legislation, such as the Telecommunications Act or the ePrivacy Directive. However, the DPA does not rule out that this legislation may also apply.

2.3 The course of the investigation

In the months of May, June and July 2020, the DPA investigated the use of online voice and video calls and online proctoring in education at 12 educational institutions. The DPA opted to focus its investigation on institutions providing secondary vocational education, higher professional education and university education, since they yielded the highest number of indications of potential issues. In addition, the easing of COVID-19 measures when this investigation was conducted meant that many primary and secondary schools would soon resume regular education on location. Nevertheless, the recommendations are also relevant for educational institutions in primary and secondary education.

In selecting the educational institutions approached, the DPA took into account the number of students enrolled and the institutions' geographical distribution within the Netherlands. The selected educational institutions were contacted in writing with the request to complete a questionnaire. This questionnaire is included as Annexe 1 to this report. All the selected educational institutions answered the questions and substantiated their answers with additional documentation.

The documentation received has been analysed by the DPA. This report presents its findings. The report mirrors sequence of the questionnaire as far as possible. The DPA has drawn on its findings to provide recommendations for educational institutions and share best practice.

2.4 Next steps

The DPA will continue to monitor developments in remote education. It goes without saying that, in addition to complaints and indications of potential issues, the DPA will also take note of court rulings and developments in other EU member states. In the short term, the DPA will enter into discussions with the umbrella organisations in the education sector about the results of this investigation. In the areas where the biggest improvements can be made, we will explicitly bring to their attention the improvements we believe are needed.

3. Findings

3.1 Use of online applications

If an educational institution chooses to use online voice and video calling applications and/or online proctoring software, the educational institution is responsible for the personal data processed in this context. As the data controller, the educational institution must be able to demonstrate compliance with the GDPR.

Legal basis
An important element of accountability is being able to demonstrate a legal basis for processing personal data. This legal basis must be determined before the educational institution starts processing personal data.

From the documents received, the DPA concludes that there does not seem to be a clear picture when it comes to determining the legal basis in so far as the education provided under the Adult and Vocational Education Act (WEB) and the Higher Education and Research Act (WHW) is concerned. Below, the DPA will highlight a number of legal bases about which confusion seems to exist in the context of remote education.

- *Public interest/official authority (public task)*
  An educational institution may invoke as a legal basis that processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller. This task must be laid down by law. It is often difficult to determine the boundaries of a public task and whether the public task provides a sufficiently accurate legal basis for certain data processing operations. Moreover, what is necessary for the performance of a public task may vary over time. For example, an educational institution may come to the conclusion that COVID-19 measures make it necessary to process video images of students in specific situations in order to carry out the public tasks laid down by the Adult and Vocational Education Act and the Higher Education and Research Act. It is important that it is clear to students that their personal data will be processed in order to perform this specific statutory task.

- *Legitimate interest*
  The GDPR stipulates that legitimate interest cannot be invoked as a legal basis for the processing of personal data by public authorities in the context of performing their duties. Educational institutions governed by public law cannot therefore rely on th is legal basis in carrying out their tasks.

- *Consent*
  In order for an educational institution to be able to invoke consent as a legal basis, a student must be able to freely consent to the processing of their personal data. Consent is deemed to be given 'freely' if students have a genuine choice and control. The relationship of authority between the educational institution and students can be problematic for any invocation of the legal basis of consent. After all, it is doubtful that students actually have the freedom to r efuse consent requested by the educational institution if there are consequences attached to this refusal. In order to be able to speak of free consent, the educational institution must at least offer an alternative to the intended data processing operation. If a student that refuses consent is unable to take lessons or sit a test or examination, consent cannot be regarded as freely given. Likewise, consent that a student is assumed to have given by participating in a digital lesson or an examination

administered using online proctoring does not constitute legitimate consent within the meaning of the GDPR.[1]

The answer to the question of which legal basis is appropriate in a specific situation when organising remote education always depends on the circumstances and the concrete purpose for the use of digital applications. In any case, it is important that the educational institution is able to justify its choice of a particular legal basis. In addition, in order to be able to successfully invoke one of the above legal bases, the processing of personal data must be necessary to achieve the underlying purpose. This will be discussed further in section 3.1.2.

Recommendation: Before processing personal data, identify the legal basis for this personal data processing and explain why it is applicable. The educational institution has its own responsibility to assess the necessity of the data processing operation.

Data protection impact assessment (DPIA)
In accordance with the accountability principle under the GDPR, educational institutions must be able to demonstrate that they have taken appropriate technical and organisational measures to protect students' personal data. One of the concrete actions mentioned in the GDPR to assess the risks of a data processing operation and to determine the appropriate measures is to conduct a data protection impact assessment (DPIA). This is mandatory in case of data processing operations that pose a high risk to the rights and freedoms of individuals.

In the investigation, the educational institutions were asked about the way in which they took the protection of personal data into consideration in choosing to use various digital applications. The DPA notes that many educational institutions have (recently) carried out a DPIA to identify the risks of the current or planned data processing operations.

As the data controller, it is up to the educational institution to determine whether a DPIA obligation applies to a specific personal data processing operation. Educational umbrella organisations could play a facilitating role in performing a joint DPIA. The DPA has drawn up a (non-exhaustive) list of data processing operations for which the performance of a DPIA is mandatory before the data controller initiates processing. Depending on the purpose and the way in which online voice and video calls and online proctoring are used, the following data processing operations on this list may be relevant in the context of remote online education:

- Large-scale and/or systematic monitoring of personal data for anti-fraud purposes.
- Large-scale and/or systematic use of flexible camera surveillance.
- Systematic and comprehensive assessment of personal aspects of natural persons based on automated processing (profiling).
- Large-scale personal data processing operations in which the behaviour of natural persons is observed or influenced in a systematic way, or data is collected and/or recorded about them, by means of automated processing.

Even if the data processing operation is not on this list, educational institutions must assess whether the data processing operation poses a high privacy risk to the data subjects. The nine criteria drawn up by the European privacy authorities can be used for this purpose. As a rule of thumb, a DPIA must be performed if the personal data processing operation meets two or more of these criteria. In the context of online voice and video calls and proctoring, the following criteria may be particularly relevant:

[1] For more information on the conditions that must be met to legitimately invoke consent as a legal basis, see the Guidelines on Consent under Regulation 2016/679.

- Evaluation of people based on personal characteristics (such as behavioural analysis using an algorithm for online proctoring).
- The sensitivity of the data that can be shared via the medium (such as religious convictions, health information or political preference).
- The large-scale nature of the data processing.
- The vulnerable position of the data subjects whose data is processed (unequal balance of power between the educational institution and the teacher/student).

When organising remote education, many of the surveyed educational institutions opted to use online voice and video calling applications that were already being used within the educational institution (sometimes for other purposes). The DPA notes that this may have been a good choice, especially in light of the external time pressure, but emphasises that when a voice and/or video calling application is used for purposes other than those for which it was initially purchased, data processing may entail different risks and a DPIA, or a new DPIA, may be required. For example, the use of a voice and/or video calling application during a meeting will have a different impact on the protection of personal data than its use to teach a class or give a lecture to a large group of students.

Performing a DPIA is not a once-and-done undertaking, but an ongoing process. It is therefore good practice to constantly review a DPIA and regularly re-assess impact.[2] A number of educational institutions explicitly stated in the documentation that was provided that they would be re-evaluating the DPIA within a set time frame or when the measures were relaxed, in part to re-assess the necessity of the data processing (see also section 3.1.2). The DPA considers this a good approach to this ongoing process that educational institutions are required to follow.

Finally, the GDPR stipulates that the data controller must, in performing the DPIA, "*where appropriate... seek the views of data subjects or their representatives on the intended processing*." The DPA accordingly views it as an appropriate implementation of this requirement for educational institutions to ask students and teachers or their representatives (such as student councils, university councils, central participation councils and/or other forums) about their views on data processing in organising remote education, even if these persons or bodies do not have any right to give a legally binding advisory opinion or right of approval.

Performing a DPIA will generally be mandatory if an educational institution plans to use voice and/or video calling applications and online proctoring. If a digital application was already being used by an educational institution, but is now used for a new purpose – such as the large-scale provision of remote education – there may be a change in the risks arising from the data processing. A DPIA, or a new DPIA, be mandatory in that case. In addition, performing a DPIA is an ongoing process. The easing of COVID-19 measures, technical developments, and other circumstances that may affect education and society in a broader sense could lead to a different outcome of this assessment.

Recommendation: Periodically check whether the DPIA needs to be reviewed, to re-assess the necessity of data processing among other things. In such cases, also seek the views of students and teachers (and their representatives).

The DPA concludes from the information received that many of the surveyed educational institutions seem to be aware of some of the risks associated with the use of online voice and video calling applications and online proctoring software. The DPIAs and other documentation provided frequently mention the risk

[2] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" within the meaning of Regulation 2016/679, p. 17.

that sensitive data on students might fall into the wrong hands. The DPA emphasises that it is important in the risk assessment to include the risks that do not result directly from a data breach. Besides breaches of student data, the use of online proctoring could also lead for example to the unjustified exclusion of students from an examination. These risks should also be included in a DPIA, where relevant.[3]

Recommendation: When performing a risk assessment, also take into account other risks that affect (fundamental) rights and freedoms, such as unjustified exclusion of pupils or students from a test or examination.

Data processing agreement

All the surveyed educational institutions indicate that they use software suppliers that process personal data on their behalf in the context of remote education. If the educational institution alone determines the purpose and means of the processing, then the software supplier is a data processor within the meaning of the GDPR. The GDPR stipulates that the data controller may only use processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subjects. It is therefore the responsibility of the educational institution to set requirements for the software companies that supply the online applications. The agreements made with these suppliers should be recorded in a data processing agreement. The DPA's investigation shows that not all the surveyed institutions had already signed data processing agreements with the software suppliers.

Besides the fact that the GDPR requires a data controller and a data processor to enter into a data processing agreement, it is important that the educational institution has actual insight into the processes of a data processor, so that compliance with the provisions of the data processing agreement can be verified. Under the GDPR, the data controller in principle remains responsible if the data processor fails to comply with the GDPR. For that reason, educational institutions must exercise due care when drawing up agreements with the supplier.

If data is processed by a third party on behalf of an educational institution as part of the delivery of remote education, the educational institution is legally required to enter into a data processing agreement with this data processor.

Recommendation: Despite the limited number of suppliers available for online voice and video calling applications and online proctoring software, be critical about whether agreements comply with the GDPR and offer appropriate guarantees for the protection of students' personal data.

International transfers

The DPA has found that many voice and video calling applications and online proctoring software solutions are offered by suppliers in the USA. Educational institutions should take into account that the GDPR requires the transfer of personal data from the Netherlands to countries outside the European Union to comply with the statutory provisions of the GDPR. This means that it is first necessary to assess if the European Commission has issued an adequacy decision for the third country, a region, or one or more specified sectors in that third country. If that is not the case, then organisations can make use of one of the transfer instruments that are specified in the GDPR, provided they offer adequate safeguards and the data subjects have access to enforceable rights and effective legal remedies. If that is not possible then personal

[3] See the European Data Protection Board's guidelines on DPIA: '(...) the reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.'

data can be transferred in exceptional cases on the basis of one of the derogations for specific situations mentioned in the GDPR, if the conditions are met.

In a recent judgment, the Court of Justice of the European Union declared the decision on the adequacy of the EU-US Privacy Shield invalid, because that decision cannot guarantee sufficient protection of personal data. For that reason, educational institutions and other organisations can no longer rely on that adequacy decision for the transfer of personal data to the United States. This means that data processors that are engaged by the educational institution to provide, for example, online proctoring services, may not transfer personal data to organisations that are based in the United States without taking additional measures to safeguard the principles of the GDPR. For more information about the consequences of this judgment, see the FAQ document on the CJEU judgment published by the European Data Protection Board.

As the data controller, the educational institution is responsible for providing a valid legal basis for the transfer of personal data to third countries, for instance by including additional measures in model contracts.

3.1.1 Online voice and video calls

All the surveyed educational institutions state that education under the COVID-19 measures is facilitated largely or partly via applications for online voice and video calls. It is apparent from the information provided that educational institutions use various applications and take various approaches to offering freedom of choice to faculties, those responsible for degree programmes, and teachers in choosing online voice and video calling applications. Several educational institutions require their employees to use digital applications that have been approved by the educational institution. The risks of these applications have been assessed, appropriate safeguards have been put in place, and a data processing agreement has been arranged with the supplier if necessary.

> *"The internal guideline is that degree programmes make use of digital teaching resources that are offered at the level of the organisation. In this context, the security and privacy risks have been assessed in advanced and minimised where necessary and possible. Moreover, a data processing agreement has been signed with the suppliers."*

Some of the surveyed organisations indicated that the degree programmes or teachers are considered responsible within the organisation for selecting a specific online voice and video calling application. The degree programme or teacher is expected to ascertain independently that the required level of protection of personal data has been achieved before starting to use the application. These educational institutions do generally recommend certain digital applications or prohibit the use of a few digital applications, and almost all indicate that data protection plays an important role in that choice. The DPA advises against making individual teachers or students responsible for choosing which applications to use, because they are not always aware of the possible risks of a given application.

As the data controller, the educational institution is responsible for determining which online voice and video calling applications are to be used in the delivery of remote education. As part of its duty to provide accountability, the educational institution must be able to demonstrate how the protection of students' personal data was taken into account in the choice of an application. By entering into data processing agreements with the suppliers of the digital applications and drafting an institution-wide policy that provides appropriate safeguards, the educational institution remains in control of the processing of personal data.

Recommendation: The DPA advises against making individual teachers or students responsible for choosing online voice and video calling applications. See our selection guide for help choosing online voice and video calling applications.

3.1.2 Online proctoring

The DPA also specifically asked the selected educational institutions about the use of online proctoring software. Online proctoring is described by ICT cooperative SURF as a form of location-independent digital testing, in which the educational institution uses software developed especially for this purpose to invigilate a test or examination to prevent fraud. This happens in part by watching video images via the student's webcam and viewing the display windows that the student has opened on their screen. Other control software options that are offered include tracking mouse movements and monitoring keystrokes. Students may also be asked to use the webcam to show their surroundings.

The available online proctoring software suppliers offer various options to analyse and assess the data that is collected. First, there is an option that an invigilator from the educational institution observes a student taking a test or examination in real-time (live proctoring). In addition, it is possible to review the video and screen recordings afterwards or have invigilators employed by the software suppliers assess these recordings (retrospective proctoring). Finally, suppliers offer the option to have the video recordings and other data reviewed automatically using an algorithm that detects indications of possible fraud (automated reviewing).

Some of the surveyed educational institutions indicated that they did not yet use online proctoring software. Most of the educational institutions that do use online proctoring are among the larger institutions, including all of the universities that were contacted. These institutions primarily opted for automated reviewing, always using human intervention to determine whether fraud has occurred. None of the educational institutions included in the investigation made use of fraud detection without human intervention.

The reasons that a few educational institutions gave for not using online proctoring include the availability of adequate alternative test formats that are less intrusive, and also concerns about student privacy and uncertainty about the effectiveness of the software. The DPA acknowledges that these are justified concerns. After all, the use of online proctoring is far more intrusive in terms of protection of personal data compared to administering an examination on location. For that reason, the use of online proctoring always requires careful consideration. The educational institution is responsible at all times for checking whether the purpose of online proctoring is proportionate to the infringement of students' privacy (proportionality) and whether the purpose cannot be achieved in some other way that is less intrusive (subsidiarity).

The DPA notes that it is not clear to all educational institutions whether online proctoring software actually detects fraud. For example, some educational institutions indicate that they cannot guarantee at this time that students cannot circumvent the technology, or could wrongfully be accused of fraud.

"The technology behind online proctoring is still under development and is still too sensitive to fraud. In addition, it represents a considerable intrusion of the student's personal living environment."

The documentation received shows that almost all surveyed educational institutions have considered alternative test formats that do not require the use of online proctoring. Alternative test formats that are mentioned include open-book examinations, essay assignments, oral examinations, and trust-based testing. In addition, various mitigating measures are mentioned that could limit the risk of fraud in tests that could not easily be replaced by one of these alternative test formats. Options that are mentioned include limiting the time to take a test, plagiarism checks, or a form of live intervention in which students are questioned by the examiner during or after a test on the basis of random sampling to double-check answers. Some of the surveyed educational institutions indicate that the available alternatives offer sufficient solutions to facilitate tests and examinations remotely without using online proctoring.

"Due to the existence of these alternatives there was no need to use proctoring – which plainly raises privacy concerns – to guarantee continuity of education."

The surveyed educational institutions that do use online proctoring or plan to do so in the near future indicate that it is not possible in all cases to adapt the test or examination so that an alternative test format can be used. This is related to such factors as:

- the number of students. Other test formats or methods of invigilation make disproportionate demands on capacity and require disproportionate effort, according to the educational institution.
- the teaching objectives of the subject. In some cases, alternative test formats do not offer sufficient insight into the student's knowledge and skills required for a subject. As an example of tests that are difficult to replace, tests that focus on reproducing knowledge are specifically mentioned.
- the role of the subject in the study programme. Certain subjects that, according to the educational institution, play a crucial role in the study programme, cannot be replaced or postponed.

All educational institutions that use online proctoring do indicate that they see it as the last possible recourse; they always consider first whether other test formats are possible.

"If there are really no alternative test formats that are feasible, or if a student specifically requests it due to personal reasons/circumstances, such as delays in a their progress or disability, then it is possible to use online proctoring – if the examination committee grants permission [...]."

In accordance with the accountability principle under the GDPR, educational institutions must keep a record of the cases in which online proctoring is used, including the reasons why it is used. Any decision to use online proctoring must be re-evaluated periodically, particularly if COVID-19 measures are relaxed.

In the context of its obligation to provide accountability, the educational institution must be able to provide good reasons why online proctoring is necessary to prevent fraud. Its decision may different from one situation to the next, depending on the nature and specific characteristics of a test of examination. The use of online proctoring should be considered a last resort. For examples of best practice on making this assessment, see section 3.2 of this report.

Recommendation: Always check first whether there are alternative test formats that represent less of an infringement of the students' personal data protection rights. Record in writing the reasons for using online proctoring for certain tests and examinations. When using automated reviewing of tests and examinations, always ensure that actual human assessment takes place.

A number of the surveyed universities have opted to regulate how online proctoring is organised according to guidelines in consultation with the examination committees. Other educational institutions that use online proctoring also indicate that they have established additional criteria to determine the cases in which online proctoring is used. Although the details of these guidelines and criteria differ between institutions, they do address the protection of personal data. For example, the regulations establish the purposes for which online proctoring is used, which forms of online proctoring are used by the university, and which parties must be involved in the event that fraud is detected.[4] These general criteria will be used to define and document any decision to use proctoring for specific tests or examinations. The DPA considers this a good way to ensure that the use of online proctoring is viewed as a 'last resort'. Moreover, it allows an educational institution to provide accountability by setting out the cases in online proctoring is used and why.[5] See section 3.2.2 of this report for examples of best practice and some suggestions regarding these guidelines and criteria.

3.1.3 The parties involved

The DPA asked the selected educational institutions about the involvement of the DPO and other parties in choosing to use online voice and video calling applications and online proctoring software. Most of the educational institutions indicate that the DPO played an active role in preparing for and/or organising remote education. Many educational institutions indicate that the DPO provided advice during the preparatory phase, was involved in performing in the DPIA, and took part formulating the privacy poli cy and related guidelines and frameworks.

"The DPO is involved in all matters that affect the protection of personal data in the broadest sense, in an advisory, controlling and initiating capacity."

Based on the answers to the questions and the documents that were received, the DPA was not able to form a clear impression of the exact role of the DPO and the point in time at which the DPO becomes involved. For instance, one of the surveyed educational institutions only notes the fact that the DPO was notified of the measures and the decisions that were taken. The DPA emphasises that it is important for the DPO to be involved at an early stage in all matters related to the protection of personal data, and should also be asked to offer advice in that context. For instance, one of the surveyed educational institutions indicated that they had actively involved the DPO as soon as they began formulating a policy on online proctoring.

Even in the operational phase after the decision-making process regarding the use of online voice and video calling applications and online proctoring software, it is important that the DPO can fulfil their supervisory role. One of the surveyed educational institutions indicated that the DPO conducts random checks of departments within the educational institutions to inquire about the necessity of using online proctoring or voice and/or video calling applications for administering a specific test. The DPO assesses the justification provided by the board as to why less intrusive alternatives are not available for this test. In addition, several educational institutions indicate that the DPO is consulted on specific questions and complaints from data subjects.

Recommendation: The decision-making process regarding the use of voice and/or video calling applications and online proctoring software and the implementation of appropriate safeguards demands timely and active involvement by the DPO. Informing the DPO afterwards about the choices that were made in the organisation of remote education is not sufficient.

The DPA also asked educational institutions which parties other than the DPO are or were involved in drawing up frameworks or guidelines about online voice and video calls and online proctoring. Besides the

[4] Based on the information received, it is not clear to the DPA whether the surveyed educational institutions have modified the teaching and examination regulations.
[5] It is not immediately clear from education legislation that an educational institution can use online proctoring and process personal data for this purpose. Drafting guidelines within an educational institution can provide more transparency about the use of online proctoring and thus contribute to the foreseeability of a data processing operation.

privacy and security officers mentioned by all those surveyed, some of the surveyed educational institutions also mentioned e.g. the participation council, student council, study programme committees, the Executive Board and the examination committees. The parties that have a right to give an advisory opinion or right of approval in relation to decisions by the Executive Board appear to have been given the opportunity to exercise those rights by the surveyed educational institutions.

Several educational institutions indicate that they have given stakeholders that are not members of an advisory body an opportunity to take part in working groups, panels or other sessions in which the participants are encouraged to provide input on how remote education will be organised.

> *"Teachers and students have been able to take part in sounding board sessions, test panels, ethical consultations and an evaluation group."*

Several of the surveyed educational institutions still seem to need to take steps in this direction. The DPA encourages educational institutions to engage in dialogue with students at an early stage and to actively involve them during the evaluation of remote education, partly in the framework of the aforementioned obligation to ask data subjects for their views when performing a DPIA. See section 3.1.

Recommendation: Do not only take into account the right give an advisory opinion and the right of approval, but also actively engage students and other stakeholders in the organisation and evaluation of remote education.

3.2 Frameworks and guidelines for educational institutions

Before educational institutions start using a digital application, it is important for them to take sufficient measures to limit the identified risks to the rights and freedoms of the individuals involved (the data subjects). An important organisational measure is developing and communicating unambiguous, clear policy on using applications and on instructing the teaching staff and students that will be working with the applications. The DPA has received indications that very different approaches to this are used by different faculties and sometimes individual teachers within educational institutions. In the framework of this investigation, the DPA requested the educational institutions to indicate which internal frameworks, rules and guidelines have been developed to handle personal data with all due care. In this section, the DPA highlights a number of points for attention and examples of best practice.

3.2.1 Secure handling of video footage

There are significant variations between the surveyed educational institutions in the degree to which they inform the teaching staff about observing all due care in handling video footage of students from digital lessons and from tests administered using online proctoring, and in the guidelines that have been drafted regarding such visual material. For instance, in response to the question about whether frameworks or guidelines had been drafted on the protection of personal data, several educational institutions only referred to general functional explanations and instructions for the use of online voice and video calling applications and online proctoring software. The DPA also received rules from various educational institutions regarding the recordings and the storage of video footage. These rules vary from warnings against unnecessarily displaying students on screen to prohibitions against showing students on screen. Similarly, the rules vary from limiting the retention period of a recorded lesson to an explicit ban on recording and saving a digital lesson.

Digital lessons

The DPA emphasises that the educational institutions as data controllers are responsible for determining which video recordings are necessary and whether they should be retained. For instance, when lessons are taught using an online voice and video calling application, and students have their camera on during the lesson, it is not permitted to save the video images of these students without good reason. However, this does not mean that the educational institution may not save and share any video footage at all from a lesson or lecture. The purpose for which the recordings are made will be the guiding principle in deciding whether it is permitted to save the video footage. For instance, the educational institution could give access to a recording of a digital lesson so it can be watched again later, without including the interactions with students in the recording. This limits how much personal data of the participating students is shared.

"Inform students beforehand if live sessions will be recorded, and only record sessions if that adds value in educational terms. Students can decide to turn off their webcam if they do not want to be part of the recording. This may not have any consequences for their presence."

An important way in which educational institutions can limit infringement of privacy is by configuring the standard settings of the online voice and video calling application so that it processes as little personal data as possible. Some of the surveyed educational institutions indicate that the camera and microphone of participating students are switched off by default during online lessons to prevent unnecessary audio and visual recordings of students. To keep a lesson interactive, students can ask questions via a chat function, for example. This is a good example of data protection by configuring standard settings (privacy by default). Drafting policy rules (no recordings of students as the default option) can help in this regard.

"The settings were configured preventively wherever possible in order to guarantee the best possible protection of personal data. These settings cannot be changed by individual users in ways that negatively affect their privacy or the privacy of other participants."

One of the surveyed educational institutions advises teachers to give asynchronous lessons. That means that the students do not watch the digital lesson live while it is being recorded, but can instead view the video afterwards. Educational institutions could consider this form of online teaching when interaction is not necessary and/or could also take place after the lesson.

If the educational institution adopts the position that making and storing visual recordings of students is necessary in order to watch a lecture again later, or for other purposes, the educational institution is responsible for explaining to the data subject why saving the recording is necessary for this purpose. In this context, teachers are advised to indicate when they are about to start the recording.

Do not make audio and visual recordings of students if it is not necessary for providing digital lessons. If it is necessary to save video footage, make sure that the reason for doing so is documented and that the individuals involved (the data subjects) are informed. Configure the standard settings of the online voice and video calling application in such a way that the processing of personal data is minimised.

Recommendation: Take into account alternative possibilities for interaction, e.g. the chat function of a voice and/or video calling application or the digital learning environment of the educational institutions. By drafting clear guidelines, it is possible to prevent video footage being handled in different ways within the same educational institution.

Remote testing

Although it will not be considered necessary in many situations to show students on screen while recording digital (theory) lessons in secondary vocational education, higher professional education and university education, a different conclusion may be reached if video recordings are to be used for administering practical assignments or oral examinations, or the context of online invigilation. Reasons mentioned by educational institutions for storing video recordings include assessment and, in the case of online proctoring, analysis of the images, and ongoing fraud investigations.

The DPA notes that educational institutions use different retention periods for storing video footage for the aforementioned purposes. Several of the surveyed educational institutions seem to base them on the storage periods offered by the supplier of the digital application, especially in the context of online proctoring. The DPA notes that video footage must only be stored for as long as is necessary for the purpose for which the personal data is processed. For instance, if online proctoring is only used for the purpose of fraud prevention and to verify the student's identity, and there is no evidence that the student committed fraud during the examination, then the video recordings should be deleted after the ID check. In addition, it will probably not be necessary to store a recording of a digital oral examination if it would normally (in an offline setting) not be necessary to record an oral examination. The storage peri ods offered by the supplier should not be the guiding principle used to determine the retention periods.

If a teacher or examiner concludes based on the instructions and guidelines of the educational institution that it is necessary to save a recording, it is important for the video recording to be stored in a secure environment. Only staff members of the educational institution who are authorised to do so may access the recordings.

"Authorisation profiles have been used to limit the group of people (invigilators and test experts) who may view recordings. Moreover, invigilators must carry out their assessment activities on a secure computer of [educational institution X] (on campus) for reasons of technical security."

One of the surveyed educational institutions instructed teachers, in a teacher guide, to record an oral examination using the audio recording function on their personal mobile telephone if they do not want to use the recording function provided in the voice and/or video calling application. This method does not give the educational institution any control over security or deletion of the audio recording, and the DPA accordingly advises against this practice.

The documentation received shows that various different persons within the educational institutions are tasked with promptly deleting stored recordings. Sometimes it is the teacher, while in other cases a central department is responsible for doing so, or the videos are deleted automatically. It is advisable to opt for a method that offers reasonable certainty that the recordings will not accidentally be stored for longer than intended. Automation may offer effective support here (e.g. automatic deletion, reminders, etc.).

If video recordings of students (in the context of a digital test for example) are stored temporarily, the educational institution is responsible for ensuring that the videos are saved securely.

Recommendation: Instruct teachers and examiners to store images only in a secure environment and ensure that the recordings are not stored for longer than necessary. Explore whether automation can play a supporting role in this regard.

3.2.2 Assessment framework for alternative testing

As stated previously in the report, all the surveyed educational institutions that use online proct oring indicate that they only use that method if no alternative form of testing is possible. Based on the information received, it is not clear to the DPA how each educational institution arrived at this conclusion and who ultimately decides to use online proctoring for a specific test.

Several of the surveyed educational institutions indicate that they encourage teachers to think about alternative test formats and measures to limit fraud. These educational institutions do not (yet) have institution-wide guidelines that address the question of the circumstances in which a specific test format can be used. It would appear that the final decision at these educational institutions rests with the teacher. Other educational institutions indicate that the assessment of whether online proctoring is used in a specific situation is made by or should be approved by other people and bodies, such as the teaching director and/or the examination committee.

As part of its duty to provide accountability, it is important that the educational institution can provide information about how it decided whether to use online proctoring. An important question that must be answered here is whether it is possible to arrive at a reliable assessment of students' knowledge and/or skills using other, less intrusive measures than online proctoring or alternative test formats.

"A decision is made based on an evaluation of appropriate alternatives, the size of the group, the nature of the test format, proper and timely communication to students, and feasibility (support). The assessment is documented, so it can be shown for each test which considerations played a role in the use of online proctoring."

The following questions are among those used by the surveyed educational institutions to determine which solution or alternative test format would be suitable for administering a test or examination remotely:

- Can the test be administered in its current form without supervision?
- Can the group of students take the test in small groups at different times?
- Can the competencies that are assessed by this test also be assessed by employing other test formats, such as an individual or group assignment or an oral test?
- Can the test be postponed?

Clear guidelines in which these and other relevant questions are explored can prevent teachers and examiners from making different assessments and arriving at different conclusions regarding the possible use of fraud prevention measures. For that reason, the DPA advises educational institutions to clearly document this assessment framework on paper. By doing so, the educational institution can comply with the requirement for demonstrable GDPR compliance.

In order to help teachers, examiners, examination committees and other relevant staff to explore alternative test formats, several educational institutions have provided a schematic overview that sets out the conditions for various test formats. The questions listed above and others could be answered using a decision tree. The answers to these questions will lead to a recommendation on what form of testing to use.

Recommendation: Ensure clear, institution-wide guidelines that instruct and support teachers and examiners to always first consider the options that least infringe students' personal data protection rights when administering a remote test or examination. Document the assessment that is made if the educational institution decides that online proctoring will be used for a specific test or examination.

3.2.3 Remote identification

One method that differs markedly among the surveyed educational institutions that administer tests remotely using video applications or online proctoring is how students verify their identity. In practice, this is often done by having the student show identifying data.[6] The DPA has reviewed various instructions. For instance, some students are asked to state their name and student ID number before taking the test, while other students are asked to show a student ID card (or university ID or campus card) or identity document on screen.

The surveyed educational institutions indicate that verifying student identity is necessary in order to prevent fraud. During a test or examination on location, this is done by having the student show the invigilator a student ID or identity document. During this check, no recording or copy is made of the ID card presented for identification purposes. During a test or examination administered remotely using video surveillance, it is not possible to show a student ID or identity document without making a copy (video recording). For that reason, it is important that educational institutions ask themselves how they can minimise the infringement of a student's right to protection of personal data as much as possible.

A student ID does not have as much (sensitive) data on it, compared to an identity document issued by the government. The DPA found that some of the surveyed educational institutions therefore instruct students that they should preferably show their student ID card for identification purposes.

"For privacy reasons, you are urged to present your campus card."

These educational institutions indicate that when it is not possible to show a student ID, for example because the student has lost it and has not yet received a new card, the student can use an identity document for identification purposes. The DPA emphasises that, when there is no other option to verify a student's identity, an educational institution may only ask the student to show a identity document with some data concealed. Making a copy (video recording) of a fully exposed identity document is only permitted if a data controller will be processing that copy for legally established purposes. It is therefore also important that the educational institution inform students that they should cover up all data that is not absolutely necessary when displaying the identity document. In any case, the citizen service number (BSN) should be concealed.

"If you do not have a campus card, you may use an official identity document. If you do so, cover up your citizen service number."

Not all of the surveyed educational institutions provide clear instructions as to how a student should provide proof of identity, what data is necessary for that proof, and what data should be concealed when showing an ID card. Clear guidelines for students and teaching staff can prevent the unlawful processing of sensitive data.

Even if the educational institution can state why it is necessary to show identity documents (with data partially concealed), and no more personal data is processed than necessary to verify student identity, recordings must be properly secured and deleted in a timely manner.

Recommendation: Make clear agreements with examiners and invigilators regarding how students provide proof of identity during digital tests. Translate these agreements into clear instructions for students. It is not permitted to have a student present their identity document with all the data visible.

[6] There are alternatives that could be used, such as unique login details for students, including two-factor authentication (e.g. a code sent by SMS text message), but it is important that the method of identification is always appropriate to the purpose for which it is being used. The purpose of the investigation was not to determine which methods are or are not 'GDPR-compliant'. In each case, that is up to the educational institution to determine.

3.3 Providing information to the data subjects

The GDPR stipulates that data subjects have a right to clear information about the processing of their personal data. In the course of the investigation, the DPA asked the educational institutions about how data subjects are notified. In this section, the DPA shares its findings on how the duty to inform is fulfilled by the surveyed educational institutions.

3.3.1 Transparency

Before personal data is processed, the data subjects must receive clear information about how their personal data will be processed. In the context of this duty to inform, the educational institution must provide information about, for instance, the personal data that will be processed, the specific purpose for which the data will be processed, the legal basis for that processing, and whether the personal data will be shared with third parties. This applies to online voice and video calls as well as online proctoring, and the various purposes for which these are used.

Besides the content of the information, attention should also be paid to the format in which the information is provided. Students (especially under 18 years old) cannot be expected to understand complicated legal jargon or to read long privacy statements. Educational institutions should therefore provide the information in an accessible manner.

The DPA has observed that most of the surveyed educational institutions provide information about the processing of personal data for the purpose of remote education in multiple and accessible ways. Examples of ways in which information is provided to students include news items, FAQ overviews, mailings, and verbal explanations by teachers before digital lessons or tests.

"Students receive the user guide and the privacy statement a few days before the proctored examination so they are informed about the privacy aspects."

To share the information with students in a clear and appealing way, several of the surveyed educational institutions have designed creative ways of presenting a privacy statement or conveying information in some other way. For instance, there are various educational institutions that have set up separate websites where students and teachers can find information about the processing of their personal data, as well as practical instructions and users guides for proper use of digital applications. One of the surveyed educational institutions has converted the information for students into a clear infographic which uses small icons to show at a glance which personal data is processed.

"Besides practical tips about secure working practices and privacy, the student can also find the code of conduct for remote teaching here [specific page about home education]."

Some educational institutions instruct teachers to actively notify students about how personal data is handled prior to a digital lesson or test. This could include announcing beforehand that video recordings will be made and stating how long the videos will be stored. One of the surveyed educational institutions has designed a template for the first slide of a presentation that the teacher can use to notify students.

The DPA notes that, although most of the educational institutions do devote attention to providing information to students, several educational institutions still need to take steps in that direction. Not all of the educational institutions that use online proctoring based on automated reviewing appear to provide information about how fraud detection takes place. This form of proctoring often involves a form of profiling within the meaning of the GDPR, in which the student's behaviour is monitored using automated methods in order to determine whether the student is displaying atypical and/or potentially fraudulent behaviour, which the educational institution will then evaluate. The educational institution must clearly communicate to the data subject that the processing is for the purpose of both (a) profiling and (b) decision-making based on the profile, even if human intervention does take place.[7] In that context, it is a good practice to also share information about the underlying logic for doing so, among other aspects.[8] It is not necessary for that purpose to provide all the information about how the algorithm works, not least because doing so could potentially undermine the effectiveness of the software, but the information should clearly convey how the decision is made.[9] For that reason, some explanation of the general behaviour monitored by the software is advisable. A number of the educational institutions have done so.

It is notable that some of the surveyed educational institutions do provide a great deal of information on data processing for online proctoring, but do not always do the same for online voice and video calls. For instance, some universities have an extensive privacy statement about online proctoring, but do not have a similar document regarding online voice and video calls. It is also important to provide transparency to data subjects about the processing of their personal data with regard to online voice and video calls, especially if the calls are being recorded.

Some of the educational institutions indicated that they have noticed a need for more information on this topic and that they will be addressing the matter.

Recommendation: Actively inform students about personal data processing prior to a digital lesson or test. Offer the information in an accessible and comprehensible way that is appropriate for the target audience. This could include preparing Q&As, infographics, etc.

3.3.2 Minimising infringement

Although educational institutions can and should do a great deal to safeguard protection of personal data, they are unable to influence every aspect of data processing. To some extent, students and teachers have an influence on the data they share during a digital lesson or test, although they may not immediately be aware of that fact. For that reason, the DPA asked the educational institutions about the extent to which students and teachers are advised by the educational institution to minimise infringement of their right to protection of personal data.

The documents provided show that many educational institutions do highlight this aspect in communications with students, especially in situations where recordings will be made (e.g. when recording digital lessons or during proctored examinations). Where possible and pe rmitted, students are asked to turn off their camera and microphone if they do not want to be recorded. If students are shown on screen, the educational institutions advise, among other aspects, that students should:

- avoid displaying on screen any sensitive matters related to religion, political preference, sexuality, health, etc., as well as information by which they could be personally identified that could be misused (e.g. financial documents);
- ask other household members not to enter the room;
- dress appropriately;

[7] Guidelines on automated individual decision-making and profiling for the purposes of Regulation (EU) 2016/679, p. 19.
[8] Ibid., p. 30: "*If the automated decision-making and profiling does not meet the Article 22(1) definition it is nevertheless good practice to provide the above information. In any event the controller must provide sufficient information to the data subject to make the processing fair, and meet all the other information requirements of Articles 13 and 14.*"
[9] Ibid, p. 30.

- in the context of online proctoring, close any programs that are not necessary for taking the examination and be aware that when a document has to be uploaded, any other files that are saved in the same folder will also be visible on the screen.

"When a user's private space is filmed, [educational institution] advises removing personal items from the room or taking them into account in determining the camera angle."

Even if images of a student are not being recorded and stored, it is important to highlight these measures to students. These situations still involve the processing of personal data. Besides instructions to limit infringements of personal privacy, many of the surveyed educational institutions also instruct students not to make their own recordings of online lessons.

The way in which these aspects are highlighted varies. In some cases, teachers are instructed by the educational institution to inform the students about these topics beforehand. In online proctoring, these aspects are often included in general instructions that are sent to students beforehand so they can prepare for the examination. These aspects are also highlighted in Q&As and other messages (including digital messaging).

Although the DPA notes that the focus is on instructing students, several of the surveyed educational institutions also address teachers in their guidelines and instructions. Teachers will also benefit from giving digital lessons in a neutral environment. For that reason, one of the institutions has appointed special coaches that actively advise teachers on their options for minimising infringements of their privacy during online video calls.

Recommendation: Advise teachers and students to provide a neutral environment in which personal items are kept out of view while they are being filmed during a digital lesson or proctored test. Instruct students to turn off their camera and microphone if these functionalities are not necessary while attending a digital lesson.

3.3.3 Rights of data subjects

Although it was not explicitly addressed in the questions asked, the DPA was also able to form an impression over the course of the investigation of how the data subjects – primarily students – can exercise their rights. Particularly in the context of online proctoring, the surveyed educational institutions that use online proctoring devote attention to the right to object to processing. The right to object within the meaning of the GDPR means that the data subject has the right to object to the processing of their personal data for "on grounds relating to his or her particular situation". That right can only be invoked if the legal basis for the processing concerns either the performance of a task carried out in the public interest or in the exercise of official authority (Article 6 (1) (e)) or legitimate interests (Article 6 (1) (f)). If a student objects, the educational institution must cease the data processing operation, unless the educational institution can demonstrate compelling legitimate grounds for the processing which override the data subject's interests or fundamental rights and fundamental freedoms. This requires the educational institution to weigh the interests of the student against those of the educational institution.[10] Under the GDPR, the right to object must be explicitly brought to the attention of the student and presented clearly and separately from other information.

"If the student persists in the objection, despite the additional information, the DPO refers them to the option of applying to the examination committee for an alternative test format."

[10] Guidelines on automated individual decision-making and profiling for the purposes of Regulation (EU) 2016/679, p. 22.

Not all educational institutions offer alternative test formats to students that object to online proctoring, even if the objection is accepted. Nearly all educational institutions indicate that filing an objection means that the student can only take the test at the next possible opportunity. Depending on how the situation develops regarding COVID-19 measures, there is a chance that the next possible opportunity will also involve online proctoring, according to several educational institutions. Moreover, if the next possible opportunity to take the test is not until later in the year, or even in the following academic year, it is also possible that it will lead to delays in the student's progress. The DPA emphasises that if the student's interests are more compelling, and the student successfully exercises their right to object, the educational institution must offer a test format that sufficiently addresses the objections (regarding privacy or other concerns). The most appropriate solution will depend on the objections that are raised. For example, it could be an option to offer an alternative test format without online proctoring, or to offer the test at a different location, if this is feasible.

Recommendation: Inform students of their right to object to personal data processing. If a student objects to online proctoring and the educational institution cannot demonstrate that the interests of the institution outweigh those of the students, the educational institution must offer a suitable alternative that sufficiently addresses the privacy concerns. This alternative should not entail any adverse consequences such as a disproportionate delay to a student's progress.

Besides the right to object and the right to be informed as discussed previously in the report, the GDPR also gives data subjects the right of access, the right to be forgotten (erasure), and the right to rectification and supplementation of personal data. The educational institution must ensure that an appropriate response can be given when students and teachers invoke these rights.

Annexe 1 – Questionnaire

1. A) Which digital tools do you use, or do you plan to use, to facilitate remote education by means of online voice and video calls and online proctoring?

   B) To what extent has the protection of personal data played a role in selecting these digital tools?

2. A) Have frameworks or guidelines been drafted for protection of personal data in the delivery of remote education using online voice and video calls and online proctoring?
   Examples include:
   - instructions to teachers regarding the use of specific digital tools;
   - guidelines or assessment frameworks to support the choice of alternative test formats to limit the use of online proctoring.

   If these frameworks or guidelines exist, please enclose them.

   B) Which parties within your educational institution are or were involved in drawing up these frameworks or guidelines about online voice and video calls and online proctoring?

   C) How has the data protection officer (DPO) been involved in setting policies for and organising the use of online voice and video calls and online proctoring to deliver remote education?

3. A) How are students and teachers informed about the way in which their personal data is processed for the purpose of online voice and video calls and online proctoring? Can you enclose an example?

   B) Are students and teachers advised on how they can minimise infringements of their privacy during online voice and video calls and online proctoring? If so, how?

AUTORITEIT
PERSOONSGEGEVENS

About the Dutch Data Protection Authority
Everyone is entitled to have their personal data handled responsibly. The Dutch Data Protection Authority supervises compliance with laws that regulate the use of personal data and provides advice on new laws and regulations.