Privacy and Ethics Reference Framework for education data

Version 1.0

Acceleration plan
Educational innovation with ICT

Secure and reliable use of education data

Privacy and Ethics Reference Framework for education data

Version 1.0

Acceleration Plan Educational Innovation with IT –
Drawn up by the Secure and reliable use of education data zone

Acceleration plan
Educational innovation
with ICT

November 2021

Contents

Summary

Responsible use of education data from the perspective of privacy and ethics

Higher education institutions in the Netherlands are increasingly using education data to enhance the quality, effectiveness and efficiency of higher education. In order to reap the benefits of education data, it is important that all stakeholders trust higher education institutions to handle data responsibly. Institutions comply with the applicable laws and regulations, but need further clarification of these rules for the use of education data.

This Dutch national Privacy and Ethics Reference Framework for Education Data (the 'Reference Framework') has therefore been drawn up under the direction of the Safe and Reliable Use of Education Data Zone of the Acceleration Plan for Educational Innovation with IT. A common framework is a tool for putting common values into practice and can contribute significantly to building trust in the institutions.

The Reference Framework concerns both the ethical principles and the legal privacy frameworks institutions should take into account when using education data responsibly. Both aspects are covered extensively in this Reference Framework.
In summary, higher education institutions should observe the following four ethical principles when using education data:

1. **Institutions are accountable for and transparent about the use of education data and they account for it.**
   Being accountable means taking responsibility. In the event of doubts about the use of education data, institutions should make it clear who is responsible or accountable. Accountability also includes the responsibility to account for the fact that education data is always used in a certain societal context.
   → 2.2.1

2. **When using education data, institutions must balance the interests of all stakeholders and data subjects in a fair manner.**
   Institutions take measures to prevent prevailing attitudes and labelling from influencing the behaviour of lecturers and students in order to avoid negative effects. A fair consideration is ensured by involving representative bodies as much as possible in the development of policy, a code of conduct or guidelines on the use of education data.
   → 2.2.2

3. **Institutions ensure that the analyses are reliable and valid.**
   Reliable and valid analyses require an approach in which the question is leading. Institutions also ensure that the use of education data is of high methodological quality. Anyone who plays a role in processing education data must have an adequate level of relevant knowledge in the field of statistics and education.
   → 2.2.3

4. **There is always room for the human factor, even where institutions use automatic processes.**
   Institutions ensure that there is always a human factor in the automated use of education data, the 'human in the loop'.
   → 2.2.4

In addition, higher education institutions pay specific attention to the following four legal privacy elements when using education data:

1. **The internal division of responsibilities is sufficiently well-defined and established.**
   Final responsibility for the careful use of education data lies with the Executive Board as the institution's daily management body. However, this does not mean that other officers do not have a role to play in prudent use of education data. End users, such as lecturers or policy officers, are the very people who need to ensure that education data is used responsibly. In addition, the Data Protection Officer (DPO) gives advice – on their own initiative or on request – and can act as a monitor within the institution. Institutions themselves identify which officers are or should be involved in the use of education data, such as a privacy officer, general and medical ethics boards, education data team, Information Security Officer/Chief Information Security Officer, and so on.
   → Chapter 5

2. **The use of education data is communicated in a sufficiently transparent way.**
   Whenever an educational institution intends to use education data, it must provide stakeholders and data subjects with all relevant information about its use, such as the purpose for which the education data will be used, whether the education data will be shared with another organisation and, if so, with which organisation, and how the individual can contact the institution in case of any questions. This is best done at the time the personal data will actually be used as education data. This can be done in a layered manner.
   → Chapter 6

3. **Data subjects are supported in exercising their rights.**
   The institution must support data subjects in exercising their rights and not create unnecessary barriers. For some data subjects, this can be provided to a certain extent through a self-service portal for students or lecturers, for example.
   → Chapter 7

4. **Institutions apply the three-pronged principle of *purpose*, *basis* and *due care* to all use of education data. The purpose is clearly defined; the basis is clear; and the standards of care are duly observed.**
   Any use of education data must have a clearly defined purpose, have an appropriate basis and all necessary organisational and technical measures have to be taken to ensure due care in using education data. This three-pronged approach also applies when providing data to or receiving data from other parties. Furthermore, if a processing operation is likely to present a high risk to the data subjects, a Data Protection Impact Assessment (DPIA) must always be performed.
   → Chapters 4 and 8

1 Introduction

Using education data requires the trust of students and staff that it will be done responsibly. This national Privacy and Ethics Reference Framework for Education Data (the 'Reference Framework') has therefore been drawn up under the direction of the Safe and Reliable Use of Education Data Zone of the Acceleration Plan for Educational Innovation with IT.

A common framework is a tool for putting common values into practice and can contribute significantly to building trust in the institutions. The Reference Framework also provides a common language for the use of education data and gives higher education institutions the opportunity to learn, from each other, how to work with education data responsibly.

This Reference Framework sets out the ethical principles and legal principles for the responsible use of education data as well as a practical guide explaining the legal frameworks that apply to education data. It indicates, where possible, how institutions can make their own considerations in this regard.

Explanation: coherence between ethical and legal approaches

Answering the question of what constitutes responsible use of education data involves both a legal and an ethical component. These two aspects are closely linked and require an ongoing dialogue about what is considered desirable in society.

For example, Article 5 of the General Data Protection Regulation (GDPR) contains the most important basic principles, such as fairness, lawfulness and transparency. However, these are not purely legal principles but also concern the ethical aspects of responsible use of personal data.

The GDPR also provides many open standards that allow organisations to make their own considerations within the framework of the law. Where new applications arise and where the law leaves room for discretionary interpretation, ethical principles can provide guidance.

The Reference Framework is primarily intended for professionals who work with education data in practice. It also aims to inform students and other interested parties about how

education data is treated. The Reference Framework will have to be used in practice in higher education. This is a rapidly-evolving practice, which is why the Reference Framework is meant to be evaluated periodically and, where necessary, improved or expanded.

1.1 Why use a Reference Framework?

There are a number of instruments that set limits on, but also offer scope for, the use of education data. The best known is the GDPR, which sets out rules on the processing of personal data. There are also a number of instruments aimed at research, such as ISO standard 20252:2019, the Netherlands Code of Conduct for Research Integrity and the Dutch Code of Conduct for Research and Statistics.

Despite these frameworks, the use of education data in practice leads to questions about the possibilities or impossibilities of using education data, for example with regard to its effectiveness, legal frameworks and the required considerations. These questions and concerns may (unnecessarily) hinder the use of education data.

1.2 Purpose of the Reference Framework

This Reference Framework is intended to help higher education institutions use education data responsibly. At the national level, it gives direction to the responsible use of education data and contributes to trust in the use of education data by higher education institutions. What is meant by education data is elaborated in more detail in Chapter 3.

In addition, the Reference Framework is a foundation for institutions to develop institution-specific policy frameworks, practices and processes for the use of education data. It also provides support for the end users of education data. Finally, it helps clarify for students, lecturers, and other data subjects and parties involved the methods by which the institution uses education data. A data subject in this context always refers specifically to the definition in the GDPR (see 3.4.4) and is often a student. When referring to someone who is involved in *using* education data, we use the term stakeholder or interested party.

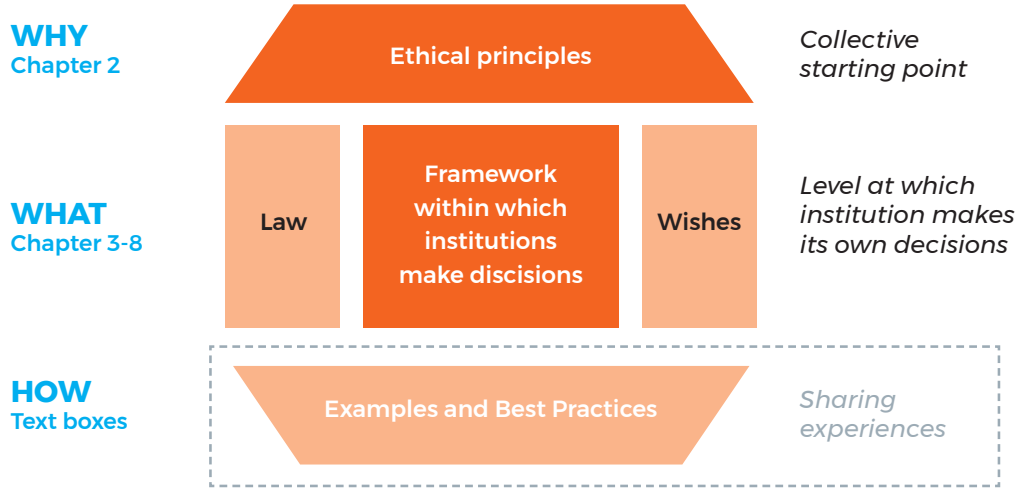
The Reference Framework is therefore intended as a guiding instrument to enable institutions to draw up their own policy, framework or code of conduct in which they lay down how they deal with education data. This Reference Framework is also development-oriented and supportive, which means that it remains possible for institutions to give their own interpretation to the use of education data.

1.3 Contents of the Reference Framework

This Dutch national Reference Framework provides the framework for the responsible use of education data. It focuses on privacy and ethics, describing on the one hand the basic ethical principles and, on the other, the legal frameworks an institution has to take into account when using education data. These include, for example, assigning responsibility for the use of education data within the institution, complying with the requirement of transparency, and supporting data subjects in exercising their rights.

Within these frameworks, the institutions themselves must give further substance to how they use education data responsibly. For example, they must decide for themselves how they will organise data governance and how students can obtain insight into their personal data.

1.4 Reading guide



Chapter 2 starts by looking at the ethical principles involved in the responsible use of education data. The ethical principles provide a common starting point for all higher education institutions and answer the 'why' of using education data. The subsequent chapters describe what is necessary to do justice to these basic ethical principles within the framework of the law. Text boxes discuss practical examples based on cases from a user group.

Chapter 3 provides the scope and definitions for this Reference Framework. First, the term education data and the applications for which education data can be used by institutions are discussed. The terms relevant to this Reference Framework are then discussed in more detail, such as privacy, personal data, special personal data, data controller and data subject. It describes what is meant by these terms and how they can be interpreted in the context of the use of education data. Chapter 4 looks in more detail at the responsibilities of the institutions, such as determining a clear purpose and ensuring that there is a legal basis. Chapter 5 discusses the allocation of responsibilities within an institution in more detail. Chapter 6 is about transparency and accountability. Chapter 7 deals with how the various rights of data subjects can be implemented in the context of education data. Chapter 8 discusses various additional safeguards and measures that can be taken by the institutions. Chapter 9 concludes with a number of paragraphs containing a brief outline of how this Reference Framework came about and the follow-up process.

2 Ethical principles

This chapter sets out the ethical principles that guide higher education institutions in the use of education data. Naturally, compliance with the applicable laws and regulations – especially those concerning privacy and the protection of personal data – is the guiding principle for all institutions. That said, not everything that is legally permissible is also ethically justifiable. Furthermore, laws and regulations provide room for individual interpretation and this, too, should be approached in an ethical manner.

Case study: wellbeing monitoring

In wellbeing monitoring, individual students' personal and social factors are recorded and analysed. This gives students insight into – and personalised advice on – ways to improve their wellbeing. The collection and use of this type of education data has both legal and ethical aspects. The considerations must be made explicit and transparent to the data subjects. Weighing up all the factors involved should answer the following questions, among other things

1. What is the institution's purpose? If the monitor is exclusively intended to help individual students gain insight into their own situation, possibly with practical tips, this will very likely lead to a different consideration and different results than if the institution also wants to use the data for meta-analyses.
2. Are educational organisations the right party to offer such help? In distance learning, those questions are likely to be answered differently than in on-campus education.
3. What is the extent of the duty of care and what does it mean for the student's autonomy?
4. To what extent does human contact concerning wellbeing issues remain possible?
5. Is the method and substantiation of the approach sufficiently valid?
6. What is the basis for this? This must include aspects such as the relationship between the student and the educational institution and the fact that, in all likelihood, this will involve the processing of special personal data.

The choices, including ethical ones, that institutions make are visible to others and feed the social debate on data and privacy. More than ever, people expect transparency, control and choice over how their data is used.[1] This is an additional motivation to describe in clear terms the actual choices made by institutions.

2.1 Digitalisation and education data

Educational institutions see great potential in the use of education data to do their work better, namely teaching, research and valorisation. Education data can be used to optimise students' intake (enrolment), progression, graduation and connection to the labour market.

The use of education data fits into a broader trend of increasing digitalisation, but is of course not new.[2] For decades, enrolment figures, examination results and educational evaluations have been useful data for higher education institutions to understand and improve their educational processes and to support their students optimally. What is changing is that the number of data sources is increasing, as is computing power and the availability of new technologies and user-friendly analytical methods.

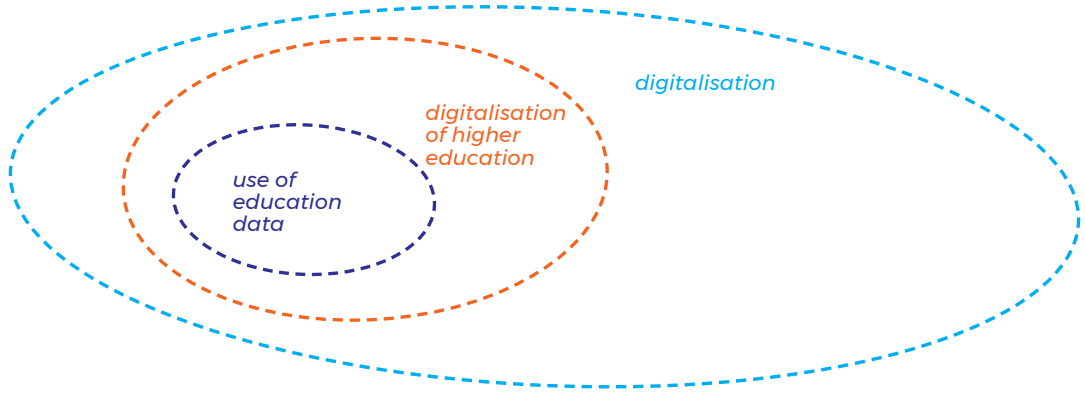
As a result, the number of possible applications for education data is also growing. Algorithms and Artificial Intelligence (AI) are being used with increasing frequency, including in the use of education data. This Framework is therefore closely aligned with the Algorithms Assessment Framework of the Netherlands Court of Audit (*Algemene Rekenkamer*) www.rekenkamer.nl/onderwerpen/algoritmes-digitaal-toetsingskader and with the value guide (in Dutch) drawn up by Kennisnet in collaboration with SURF (www.surf.nl/publieke-waarden).

These developments raise questions and concerns of an ethical nature. More and more is possible, but what are the consequences of these new possibilities? What do higher education institutions consider responsible? To answer that question, it is useful to make a distinction between digitalisation in general, digitalisation in education and the use of education data. This will make it possible for this Reference Framework to address the question of what constitutes responsible use of education data as specifically as possible.

[1] This realisation has also penetrated the marketing departments of multinationals, for example. See: Data Ethics of the World Federation of Advertisers, wfanet.org/leadership/data-ethics

[2] The use of education data involves various activities and includes the entire chain of collection, enrichment, analysis, application, presentation, visualisation, reporting, communication, storage and, finally, erasure.

Digitalisation is a process that spans a large part of society, for example, in the development of smart cities and connected cars.[3] Digitalisation in higher education falls within the general trend of digitalisation seen in society and includes all applications of and interaction with digital technology in education. This includes, for example, the digitalisation of teaching materials, the application of cloud technology and the use of social media.[4] The use of education data is a subset of the broader topic of digitalisation in education.



Case study: distance learning

The digitalisation of education is not only about what is possible and what is allowed, but also about what an institution wants: what role should IT play? Distance learning was necessary during the COVID 19 pandemic, but technology for distance learning can also be used as a source of education data. Distance learning may put pressure on some of the core values of higher education, such as humanity, justice and autonomy.

Not every student is in a position to participate effectively in distance learning, for example, because of the home situation. This increases inequality of opportunity and thus has consequences for the value of justice. And although there is often more digital contact between lecturers and students, both groups miss the day-to-

[3] See, for example, the data strategy of the Municipality of Amsterdam, www.amsterdam.nl/wonen-leefomgeving/innovatie/de-digitale-stad/datastrategie/

[4] The ethical aspects of digitalisation in education are discussed in Waarden Wegen (Weighing Values), a publication by Kennisnet, www.kennisnet.nl/app/uploads/kennisnet/publicatie/Kennisnet-Ethiekkompas-Waardenwegen.pdf

day, human contact. When using distance learning, whether for the purpose of collecting education data or otherwise, institutions will need to be accountable for the considerations they make in relation to these types of ethical questions.

2.1.1 Potential negative consequences

Digitalisation can lead to unintended and unwanted negative consequences. It is therefore important for this development to be guided by values. The Values Guide (*WaardenWijzer*) drawn up by SURF and Kennisnet (www.surf.nl/publieke-waarden) provides a common language for educational dialogue on digitalisation and the importance of educational values. When using education data, consideration should be given to possible negative effects, such as:

- Loss of the human touch, such as autonomy and the right to self-determination, the freedom to make one's own choices and the opportunity to fail: changing from a learning environment to a performance environment;
- Enabling excessive or unnecessary monitoring of students (insight into behaviour, living and learning patterns);
- Risk of educational institutions becoming less inclusive and of increasing inequality of opportunity by excluding certain groups on the basis of available data;
- Exclusion or discrimination of groups through profiling; and
- Misunderstandings due to misuse or misinterpretation of data.

Case study: Learning Management System

A Learning Management System (LMS) provides lecturers with a standard report on students that categorises their performance on the basis of two variables: 1) the level of activity (in the LMS) and 2) the results on interim assessments so far. This is visualised in an activity & grade matrix. Because this representation can lead to misinterpretations, it is advisable to ask the following questions when using this visualisation matrix:

1. Do the variables actually yield the insights they appear to give? Are they put into practice in the correct manner?
2. Is the method valid? Are the variables sufficiently predictive?
3. Is the visualisation unambiguous? Does it convey the information correctly? How do users ensure that this visualisation is put into context appropriately (e.g. by providing a clear explanation)?

The risk of negative effects increases as more data is collected without proper consideration of the purpose for which education data is used, for example:

- Browsing data 'because it is possible', without considering beforehand why, how and what consequences this will have.
- Using IT applications as an end in themselves, rather than as a means to a (higher) end.

Responsible use of education data means, in short, enabling positive interventions in education while minimising negative consequences. The principles applied by higher education institutions in this respect are detailed below.

2.2 Principles of using education data

Higher education institutions form learning communities in which students and staff have room for learning – including by making mistakes – and investigating. These are open communities in which everyone counts and feels safe to make their own choices independently. Transparency, integrity, diversity and inclusiveness are part of the public values shared by higher education institutions across the sector and are inextricably linked to the task of higher education institutions in our society.

These core values, shared by all institutions, can be put into practice in various ways. On the basis of the interviews, answers to the questionnaire and reviews with a large number of parties in higher education, the following ethical principles emerged as the most important for the use of education data:

- Accountability: *Institutions are accountable for and transparent about the use of education data and they account for it.*
- Fair consideration (equitable): *Whenever using education data, institutions must balance the interests of all stakeholders and data subjects in a fair manner.*
- Valid and reliable analysis: *Institutions ensure that the analyses are reliable and valid.*
- Human factor in automated processes (people-centred and autonomous): *There is always room for the human factor, even where institutions use automatic processes.*

2.2.1 Accountability

Transparency is an ethical principle which, within this Reference Framework, is considered one of the guiding principles for daily practice. Transparency means, among other things, that it is clear to others which data was used as a basis, how it was obtained, what results were achieved and by what means. Statutory privacy aspects regarding transparency are elaborated in the GDPR. The GDPR stipulates *what information* must be provided and *when*. Institutions decide for themselves how they share the information (see also Chapter 7).

Being accountable means taking responsibility. In cases of conflicting interests or principles, it is important to make a careful and fair consideration. In the event of doubts about the use of education data, institutions should make it clear who is responsible or accountable. More on the internal division of responsibilities can be found in Chapter 5.

Accountability also includes the responsibility to account for the fact that education data is always used in a certain societal context. Institutions are accountable for how useful and necessary their use of education data is and how they have considered the legitimate interests of data subjects and any other stakeholders.

In this context, the first consideration that institutions must make is whether a particular purpose for using education data is in line with the institution's core values and its role in society. Furthermore, institutions should document – on behalf of the data subjects – what is done with which education data and for what reason. This information should be comprehensible and accessible to the data subjects, with no barriers.

Finally, in the interests of accountability, institutions must assess whether the desired purpose has been achieved.[5]

Accountability for what can and cannot be done with education data is not a one-way street. Students and other data subjects can expect the institution to actively involve them in the choices concerning the use of their education data and – where relevant – to proactively inform them about the results. In this way, institutions maintain an ongoing dialogue with all data subjects and thus contribute to promoting a culture using data responsibly.

2.2.2 Fair consideration (equity)

Any use of education data requires a fair weighing of the institution's interests in using that data and the potential impact on the data subjects, often the students. Education data should only be used to support higher education institutions' role in society. The use of education data must have a positive purpose, that is, it must be beneficial to the quality, effectiveness and efficiency of education and education policy, the provision of education with appropriate counselling for individual students, and be conducive to research and valorisation.

In doing so, the institution carefully considers the possible adverse effects on individual students or groups of students. Consider, for instance, promoting and safeguarding diversity and inclusiveness. Institutions ensure that the use of education data does not lead to unintended discrimination against groups. The use of education data supports an active diversity policy that contributes to reducing inequality, removing barriers and ensuring equal opportunities for all.

Institutions take measures to prevent prevailing attitudes and labelling from influencing the behaviour of lecturers and students in order to avoid negative effects. A fair consideration is ensured by involving representative bodies as much as possible in the development of policy, a code of conduct or guidelines on the use of education data.

A fair consideration is further ensured by involving the participation body as much as possible in the development of policy, a code of conduct or guidelines on the use of education data, at least insofar as this is mandatory. Taking the concerns and any wishes of students and lecturers into account in a timely manner enhances responsible use and increases trust in the use of education data by the institution.

2.2.3 Reliable and valid analysis

Valid and reliable analyses start with a clear question. It calls for reflection before starting the process of collecting data. What question do we want to answer by using education data? What types of quantitative and qualitative information are required for this? The principles of necessity and proportionality are the determining factors here. Which data is really necessary for the desired purpose? Can the purpose be achieved with less or different data? Can the purpose be achieved in any other way?

Institutions also ensure that the use of education data is of high methodological quality. Individuals who play a role in processing education data should develop an adequate level of relevant knowledge in the field of statistics and education.

All algorithms and statistics used, including AI, for activities such as predictive analysis or intervention are understood, validated, assessed and, where necessary, improved by qualified staff.

Main points to consider when processing education data are:

- Inaccuracies in the data are understood and minimised;
- The implications of incomplete data sets are clear;
- An appropriate set of data sources is used;
- Anonymisation and pseudonymisation techniques are understood and correctly applied (see 8.3.1. for an explanation of these concepts);
- False correlations are avoided;

[5] The Plan Do Check Act (PDCA) cycle can be used to do this.

- Results of previous studies are taken into account;
- The results are tested for confirmation bias, self-fulfilling prophecy or other forms of bias; and
- The processing, analysis and utilisation of education data is always seen in a broader context and, where necessary, combined with other knowledge and approaches.

Important issues for the institutions are:
- An adequate level of training of staff working with education data;
- A careful and timely communication of the results to the relevant stakeholders; and
- Constant reminders about the responsibility of staff working with education data.

2.2.4 Human factor (humanity and autonomy)

The use of education data allows institutions to carry out their tasks more effectively. It is important to keep an eye on the human factor and the autonomy of data subjects. This applies in particular when education data is used in an automated way, for example with the use of AI. Institutions ensure that there is always a human involved in the automated use of education data, the 'human in the loop'. This applies in the case of automatic processes that may affect individual students or small groups of identifiable students. However, it also applies to control of the input, operation and output of the algorithms and other forms of AI used. A data subject must also have the possibility of objecting to an automated (or partially automated) decision.

Automated use of data, especially where algorithms and other forms of AI are used, does not mean the institution is not responsible for the input fed into the algorithm, what happens in the algorithm and what is produced by the algorithm. On the contrary – an institution is also responsible for using algorithms and AI correctly, carefully and fairly.

Procedures for processing, analysing and using education data and interventions are therefore carefully designed and regularly reviewed. In this context, institutions also recognise that automated analyses of education data probably cannot give a complete picture of a person's learning process and that personal circumstances cannot always be included. The institution should also be able to explain why and on what basis certain choices are made, whether these are policy choices or choices that affect an individual directly, and to do this on a regular basis. Moreover, the use of new (but also existing) techniques should never be a goal in itself, but a means to achieve a higher purpose.

3 Scope and definitions

This chapter first examines what is meant by education data and for which applications education data is most commonly used by higher education institutions. This is followed by a discussion of the relevant concepts relating to privacy and the protection of personal data.

3.1 Education data

The concept of education data used in this Reference Framework encompasses different types of information used for the purpose of improving the quality, effectiveness and efficiency of higher education. This includes providing management information, developing education policy, conducting educational research and promoting student success, where necessary through individual interventions. It is not limited to information about students only, but can also include information about lecturers and other data subjects or education information.

No type of data or personal data is education data in itself or collected specifically for that purpose. But all information (often a mix of information) held by a higher education institution can potentially be used as education data.

The specific processing of the information and the purpose of such processing therefore determine whether the information falls within the concept of education data.

For the context of the Reference Framework, a broad notion of education data is applied, including big and small data sets, structured and unstructured data, data from administrative systems as well as management systems, and both historical and real-time data. This Reference Framework applies in particular to education data that can be traced back to individual persons.

3.2 Applications of education data

Within the institutions, education data is used by administrators, programme directors, lecturers, support staff, policy officers, student counsellors and researchers who, each from their own role, use education data to improve education. Students themselves also make

use of the insights offered by education data.[6] Analyses with education data are also interesting and relevant for parties outside the institutions, such as policymakers at national, regional and local governments and supervisory authorities such as the Education Inspectorate.

In the context of the use of education data, the terms 'learning analytics', 'student analytics', 'business analytics' and 'predictive analysis' are frequently used. However, not all institutions interpret these terms in the same way. Moreover, some institutions use their own terminology to describe what they use education data for in their institution. To avoid confusion, this Reference Framework does not use specific terms but refers to the potential applications. These are:

- Individual interventions;
- Improving the quality, effectiveness and efficiency of education and education policy; and
- Academic education research.

Institutions must decide for themselves which applications they intend to use education data for and whether they wish to attach a specific term to this that is appropriate for their own institution.

3.2.1 Individual interventions

In some cases, education data can be used for individual interventions or interventions aimed at a small group of students whose identity is known or traceable. This will be done mainly to provide better counselling to the student or a small group of students with the aim of advancing their study success.

3.2.2 Improving quality, effectiveness and efficiency of education, education policy and management information

Education data can also be used to improve the quality, effectiveness and efficiency of education or education policy, or for management information. This may be useful, for example, to optimise the intake, progression and graduation/outflox of students in all phases of education, as well as to gain insight into the factors that play a role in student success. This focuses on gaining group insights and not on gaining insights into the performance of individual students, either now or in the future.

[6] A description of the benefits of data-driven work for higher education institutions is beyond the scope of this paper. For a summary of the possibilities for different target groups, please refer to: doe-meer-met-studiedata.nl/

3.2.3 Academic education research

Under certain circumstances, education data can be used for academic research, for example on study completion, study success or to review the quality of education, for example if researchers want to find out which teaching method leads to the best results.

In detail: academic research and the GDPR

According to the GDPR, academic research should be interpreted broadly and includes, among other things, academic research for the purpose of technical development and demonstration, basic research, applied research and public health studies in the public interest.

It is also recognised that academic research can be financed from private funds. However, data processing for academic research purposes must meet specific conditions, in particular as regards the publication or other disclosure of personal data for academic research purposes.

In detail: Netherlands Code of Conduct for Research Integrity

The Netherlands Code Conduct for Research Integrity has a similar scope as the GDPR, namely academic research in the broad sense, as carried out at the institutions that subscribe to the code, including VSNU, VH and KNAW. Academic research includes both publicly and privately funded and both fundamental and applied research. Research is understood to mean all activities related to research practice, such as preparing applications, designing and implementing research, assessments and peer review, acting as a subject expert, reporting, accountability and publicity.

This Code of Conduct sets out the standards for good research practice. It also lists standards that are relevant in the context of diligent use of education data for academic (educational) research. These include the following standards contained in the Code of Conduct:

- Make sure the required permissions are obtained and that an ethics review takes place if necessary.
- Describe the data collected and used for the research honestly, carefully and as transparently as possible.

- Take into account the interests and wellbeing of test persons, test animals and the risks for researchers and the environment, observing in any case all relevant legal requirements and codes of conduct.
- Be transparent about the method and procedure followed, and record them where relevant.

3.3 Privacy and the protection of personal data

This section elaborates on cases in which the Reference Framework applies. This includes an interpretation of the most important concepts in the context of the responsible use of education data from the perspective of privacy and ethics.

Privacy is a pluralistic concept. What is understood by the term privacy may differ from person to person, country to country or culture to culture. This makes it difficult to define privacy and enshrine it in laws or regulations.

The European Charter therefore does not provide for a right to privacy, but for the right to 'respect for private and family life' and the right to 'the protection of personal data'.[7] The former includes the right to respect for home and communication (e.g. the secrecy of letters). The second is the right to protection of personal data, which largely overlaps with the right to respect for private life.

The right to protection of personal data is further regulated in the European Union by the GDPR. In part, the GDPR contains open standards that allow organisations to make their own considerations regarding the responsible use of personal data. Take for instance the standard that 'appropriate security measures' are taken; what is appropriate here depends on many different factors, including the organisation, the data subjects, the nature of the data and the way in which the data is processed.

In addition, the GDPR gives the EU Member States room to elaborate on certain topics in national legislation. This gives Member States room to expand on certain points specifically for the national context. In the Netherlands, these further provisions are laid down in the GDPR Implementation Act (Dutch acronym: UAVG). This legislation sets out, for example, the exceptions that apply in the Netherlands to the use of special personal data for academic research (see also 3.4.1.). Accordingly, the GDPR and the UAVG are authoritative for this Reference Framework when it comes to the processing of personal data.

[7] See Articles 7 and 8 of the Charter of Fundamental Rights of the European Union..

3.4 Relevant terms from the GDPR and UAVG

The following terms from the GDPR and the UAVG, in particular, are relevant to this Reference Framework:

- Processing;
- Personal data and special personal data;
- Data controller; and
- Data subject.

3.4.1 Processing operation

A processing operation is any operation that relates to personal data, whether or not it is performed automatically. This includes the collection, organisation, retrieval, storage and combination right up to the destruction of personal data.

In this Reference Framework

In the context of responsible use of education data, this concerns all operations with data (personal or otherwise) used for education data. This includes the selection, collection, storage, combination, enrichment and destruction of the data.

3.4.2 Personal data and special personal data

PPersonal data is all data, or rather all information, on an identified or identifiable person (also called the data subject, see 3.4.4). This must always be a natural person, i.e. a person of flesh and blood who is still alive. Information concerning deceased persons is personal data only insofar as it relates to someone else, e.g. next of kin. Information that relates to legal persons, such as public institutions, companies or foundations, is not personal data.

Personal data may include any information directly or indirectly leading to the identification of a person. This may be information that directly or indirectly identifies a person, such as a name or an identification number, but also one or more elements that together identify a person. It will therefore partly depend on the context whether certain information constitutes personal data or not. In practice, almost all information that can be traced to an identifiable person must be considered personal data.

Processing 'ordinary' personal data is permitted, provided the requirements of the law are met, such as formulating a well-defined purpose, having a basis for processing and taking appropriate protective measures. This three-pronged approach is elaborated in the next chapter. Processing 'special' personal data, however, is generally prohibited, with a limited number of clearly defined exceptions.

Special personal data

Special personal data is personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic data, biometric data with a view to unique identification of a person, data concerning health or data concerning a person's sexual behaviour or sexual orientation.[8] BSpecial personal data may not be processed, unless the data subject has given their explicit consent or another exception applies which is provided for by law.[9]

The UAVG states that the prohibition does not apply to the processing of special personal data for academic or historical research purposes if *all* of the following conditions are met:

1. Processing the data is necessary for the purposes of academic or historical research;
2. The research serves a general interest;
3. Obtaining explicit consent has proven impossible or requires a disproportionate effort; and
4. Safeguards are in place to ensure that the privacy of the person concerned is not disproportionately affected.

In this Reference Framework

As stated in the previous chapter, the concept of education data encompasses all different types of information that are used to improve the quality, effectiveness and efficiency of education. This is not limited to information about students but can also include information about lecturers, other data subjects or educational information.

In principle, special personal data may not be used as education data. This is only possible if explicit permission is given by the relevant data subjects. Even if education data is used for academic or historical research, special personal data may be processed subject to the conditions set out above.

[8] This is an exhaustive list, see also Article 9(1) GDPR.

[9] The general exceptions to the processing prohibition are listed exhaustively in Article 9(2) GDPR and the exceptions that apply specifically in the Netherlands are listed in the UAVG.

In detail: academic research, valorisation and policymaking

Academic research using personal data, for example from test subjects, yields insights. An institution can valorise these insights as part of the policymaking process. If the insights themselves no longer involve personal data, for example because they have been sufficiently aggregated or because examples or cases have been completely anonymised (see also 8.3.1.), they can be used for policy purposes without the institution having to meet specific requirements. This is because the insights do not contain any personal data.

If the results of the academic research, including the insights, still involve personal data, it is not automatically permitted for an institution to use these results for policy purposes. In this case, the compatibility of this further use of personal data for policy purposes with the original use of the personal data for academic research will have to be assessed (see more on purpose limitation and compatible use in the next chapter).

Finally, for the purpose of conducting academic research, special personal data may be used under certain circumstances, as described above. If the results of the academic research – including insights and ensuing policy recommendations – also contain special personal data, these may, in principle, not be processed any further for policy purposes. If the insights do not contain any personal data, these insights can be used for policy purposes.

National identification number

A national identification number, in the Netherlands the Citizen Service Number (BSN), is not regarded as special personal data, but its use is subject to strict rules. The BSN may only be used for specific purposes stipulated by Dutch law and not for any other purpose. Institutions must process the BSN for the purpose of enrolment and communication with government authorities. Institutions are not permitted to use the BSN for other purposes, including for education data or as an identifier to link databases or files.

In detail: student number

A student number is not the same as a national identification number. Nevertheless, it constitutes personal information that is inextricably linked to the student during the period of study (and possibly for some time afterwards).

While the use of a student number does not fall under the strict regime of the BSN, it is important when using a student number to give sufficient attention to safeguards for the protection of the student.

3.4.3 Data controller

The data controller is the natural or legal person, public authority, agency or any other body that determines the purposes and means of processing personal data, alone or in association with others. In other words, the organisation that decides, either alone or together with other organisations, that personal data is to be collected, what it is collected for and it is to be collected, is the data controller. This organisation is ultimately responsible for the proper and lawful handling of personal data.

When two organisations cooperate and jointly determine which personal data should be processed, for what purposes and in what manner, they are called joint data controllers (for more information, see 8.2). Joint data controllers must agree on the division of tasks and responsibilities among themselves and must make the essential elements of these agreements known to the data subjects. They must also clearly indicate how the rights of data subjects can be exercised and who provides the relevant information to data subjects (see also 8.3).

In this Reference Framework

This Reference Framework concerns the responsible use of education data by (staff or researchers associated with) higher education institutions in the Netherlands. For the purpose of using education data – more specifically for the purpose of using personal data as education data – the institution is the data controller. What this responsibility entails and how it can be fulfilled are discussed further in the following chapters.

In detail: data controller and responsibilities

The institution is the data controller within the meaning of the law. Employees of an institution are not data controllers in their own right when they use personal data as part of their work for the institution, but they do act on behalf of the data controller. Chapter 6 looks more closely at the internal division of responsibilities.

3.4.4 Data subject

The data subject is the natural person who can be identified, directly or indirectly, by specific identifying elements or numbers or by one or more elements which, when combined, distinguish that person's identity. A data subject is a living person of flesh and blood to whom the personal data relates. The data subject may also exercise certain rights with regard to their personal data; see more on this in Chapter 7. If it concerns the use of data pertaining more than one natural person, the term used is (multiple) data subjects.

Explanation: use of the term 'data subject'

The data subject is the legal term used to describe the person to whom the personal data relates. In this Reference Framework, the term *data subject* will therefore also have this meaning. Where this Reference Framework refers to one or more persons who have an involvement or interest in the use of education data, we refer to them as *stakeholders*.

In this Reference Framework

Data subjects in the case of education data are students, prospective students, interested parties, former students, lecturers, counsellors and all other persons whose personal data is processed by higher education institutions. Although education data mostly concerns the data of students, it may also concern the personal data of lecturers and others. In addition, personal data may also include data on courses, curricula and study programmes taken by a student or taught by lecturers as well as data on educational institutions, faculties and academies to which the data subject is affiliated.

In detail: ‘ownership’ of personal data

When it comes to personal data, the term ‘ownership’ can lead to confusion. This Reference Framework therefore no longer uses this term but focuses instead, particularly in Chapters 4 and 5, on who the data controller is for the personal data, what their obligations are and how the internal division of responsibilities can be organised.

In practice, however, some institutions will have ‘data owners’ who are charged with managing a particular dataset and therefore have certain responsibilities with regard to that dataset. These persons can also be seen as administrators of a certain dataset, or data stewards.

This does not, however, mean that the person responsible for a dataset is also the ‘owner’ of it in a legal sense. Neither the data subject nor the institution is legally the ‘owner’ of personal data. After all, students cannot decide whether or not to provide their account number to an institution, for example; they must do this so that tuition fees can be collected. In turn, an institution may not simply decide to whom it will provide a student’s bank account number. The institution may do so only if permitted by law.

4 Responsibilities of institutions

As an organisation, the higher education institution is the data controller within the meaning of the GDPR and UAVG for the processing of personal data, including education data. This means that the higher education institution has certain responsibilities, the most important of which are elaborated in this chapter. In essence, these can be broken down into three elements and corresponding questions.

PURPOSE
Why do you want to process personal data?

BASIS
What is the legal basis for this processing?

DUE CARE
How will you ensure that you treat the data with due care?

The above requirements, which largely follow from the GDPR, are elaborated in more detail below.

4.1 Purpose

All data must be used for a clear and well-defined purpose and may not be processed further for other purposes. This means, first of all, that it must be established why personal data is to be collected and used. This may, for that matter, concern several purposes simultaneously. The purpose or purposes should be formulated as specifically as possible.

Before personal data can be used for a purpose other than that for which it was collected, it should be assessed whether the new purpose is compatible with the original purpose. To assess whether there is a compatible use, the institution itself must weigh up the situation. In this assessment, aspects such as the original and the new purpose, the context in which the data was obtained, the nature of the data, the nature of the use and the possible consequences of further use for the data subject must at least be taken into account. If a new purpose is incompatible, the data may not be used again for the new purpose unless the consent of the data subject or data subjects has been obtained for its use for the new purpose.

In this Reference Framework

The use of education data is, in reality, always about further processing of data. For this reason, it must first be made clear what purpose is served by the use of education data, and this

purpose must remain the guiding principle in its use. The purpose must be described as specifically and precisely as possible. Merely referring to the general goals of improving education, education policy, conducting educational research or carrying out individual or small-scale interventions is not specific enough.

In addition, the extent to which using the data for this purpose is compatible with the original purpose for which the data was collected will have to be assessed. Whether a new purpose is compatible requires consideration by the institution (or end user within the institution), taking into account the context and nature of the use, the nature of the data and the potential impact on the data subjects. If the purpose of processing is to send students a monthly faculty newsletter, it will probably be compatible to use the data to send a one-time information email about such events as the appointment of a new dean, for example.

In detail: academic education research as a purpose

If education data is to be used for academic educational research, the GDPR states that it may, in principle, be assumed that this is compatible use. However, to ensure that education data is actually used responsibly, a clear purpose for processing the data is required and appropriate safeguards must still be implemented. Furthermore, the expectations of and consequences for the students concerned must also be taken into account.

4.2 Lawful basis

For the processing of personal data to be lawful, it must be based on one of the six grounds provided for in the GDPR. These are as follows:

- Consent
- Necessary for the performance of a contract (contract)
- Necessary to fulfil a legal obligation (legal requirement)
- Necessary for the protection of the vital interests of the data subject (vital interest)
- Necessary for a task in the public interest or exercise of public authority (public interest)
- Necessary for the legitimate interests of the data controller or a third party (legitimate interest)

There is no hierarchical order between these grounds. There should, however, be a basis for the processing of data and it should be appropriate to the processing operation Which basis is most appropriate will also depend on the purpose of the processing operation.

In the context of education data, the most common bases are ‘consent’, ‘public interest’ and ‘legitimate interest’. The conditions and requirements for these three bases are explained below.

4.2.1 Consent

Consent must be given freely, knowledgeably, specifically and unambiguously. This means that the data subject should have all the information needed to make an informed choice about whether or not to consent to the intended processing of personal data. This consent must also be unambiguous in that there should be no doubt that the person’s consent has been given. This does not always have to be written consent. Other forms are also possible, as long as it is clear and demonstrable that consent has been given. The onus is on the data controller to prove that consent has been obtained.

Consent must also be freely given, which means a person must be completely free to make a choice. The data subject must not feel any pressure or be in a hierarchical relationship with the data controller which could affect the data subject’s freedom of choice. There should be no negative consequences whatsoever for withholding consent and the data subject must also be able to withdraw consent at any time.

4.2.2 Public interest

To apply the basis that processing of personal data is ‘necessary for performing a task in the public interest’, it must be established by law which organisation has this task and preferably also the purpose of the processing of data, the data subjects, the categories of personal data necessary for this purpose, as well as the retention periods, limitation of purpose and the entities to which the data is provided.

That law must, furthermore, seek to serve a purpose in the public interest and the processing must be proportionate to the purpose sought.

It should also be the case that using the data is indispensable for performance of the task in the public interest. This requires the organisation to assess which data is truly indispensable to achieve the stated purpose. In addition, it should be the case that the purpose cannot be achieved by other, less intrusive means, and it should be assessed whether it is appropriate or proportionate for the data to be used for the purpose sought.

4.2.3 Legitimate interest

When using the ‘necessary for the protection of legitimate interests’ basis, the interests of the organisation must be weighed against the interests, rights and freedoms of the data subject or data subjects. Elements to be considered when weighing up these interests

include the nature of the data, the category of data subject, the relationship between the data subject or data subjects and the controller, and the possible consequences of data processing for the data subjects. The weighing of interests must be documented and, where appropriate, communicated to the data subject.

In this Reference Framework

Which basis is most appropriate for the use of education data will depend on the application and the specific institution. For each instance of using education data, the institution will have to assess which basis is most appropriate for that particular instance. For certain applications and for certain institutions, for example, it will make more sense for education data to be used for the purpose of performing a task in the public interest. For other applications and/or institutions, however, it will be more appropriate to weigh up the interests on the basis that the use of education data is necessary to protect legitimate interests.

When explicit consent is the basis or exception chosen, the requirement that consent has actually been freely given must specifically be taken into account. If negative consequences are attached to withholding consent, there is no free consent. Even if the student or employee feels they cannot refuse because there is a dependency relationship between the student or employee on the one hand and the institution on the other, there is no free consent.

4.3 Due care

Due care is understood to mean all obligations on organisations that process personal data to ensure that they handle data in a responsible manner.

First of all, it is important for all data processing to be done properly, lawfully and transparently. Proper data processing presupposes that data processing does not disproportionately infringe on a person's fundamental rights and freedoms. If a processing operation leads to discriminatory actions by a data controller, for example, this is improper data processing. Lawful means that the data processing is in accordance with the law. The transparency obligation is discussed in more detail in Chapter 6.

In addition, the following principles must always be observed for processing data with due care:

- Data minimisation; only personal data that is necessary may be processed. If it is not or no longer necessary to use directly identifying data, the data must be pseudonymised as soon as possible. This applies in particular to personal data processed for historical or academic research purposes.

- Correctness; the personal data being processed must be correct.
- Retention periods; personal data may not be retained for longer than is necessary for the purpose. Insofar as necessary for historical or academic research purposes, data may be stored for longer periods provided that appropriate technical and organisational safeguards are in place.
- Security; appropriate technical and organisational measures must be taken so that personal data is processed in a way that ensures its adequate protection.

A number of these principles of due care are detailed in the following chapters.

5 Internal division of responsibilities

As a legal entity, a higher education institution is the data controller for the processing of personal data, as set out in Chapter 4. People working for or at a higher education institution are therefore not considered to be data controllers within the meaning of the law. However, they do act on behalf of the institution in performing their duties. Therefore, staff and researchers associated with a higher education institution who work with education data do play a role in using education data responsibly. The institution must determine and record who bears what responsibility for decisions relating to education data in an institution.

Higher education institutions differ from each other in size, culture, history, ambitions and vision, so there is no one-size-fits-all solution for determining and recording the responsibilities of the various officers involved. However, it is should be clear within an institution who plays which role when making legal and ethical considerations and decisions on the use of education data.

How these responsibilities are laid down internally is not specified in laws and regulations. The only matters regulated in the GDPR are under what circumstances a Data Protection Officer (DPO) must be appointed and what this officer's position and duties are (for more on the DPO, see 5.2.2).

That is why this Reference Framework takes a closer look at final responsibility for the considerations regarding education data, the officers who play a role with regard to responsible use of education data and the ways in which responsibilities can be divided.

5.1 Final report and financial accounts

Final responsibility for almost everything that happens within a higher education institution lies with the Executive Board as the institution's day-to-day management body. This also applies to the use of education data. The Executive Board can delegate certain responsibilities to another officer, such as a dean or director, through delegation or mandate arrangements.[10] It is not unusual for the education sector to make use of such arrangements, although they are hardly ever made public.

[10] At research universities, deans also have independent (attributed) powers under the Dutch Higher Education and Research Act (WHW).

In detail: delegation and mandate arrangements

The central government makes extensive use of delegation and mandate arrangements; these can be consulted on the government website.

Delegation involves the actual transfer of powers, including responsibilities. In the case of a mandate, there is no transfer of power and the mandator can therefore always continue to exercise its powers.

In practice, however, the Executive Board will not (often) be directly involved in each specific use of education data. To ensure that the higher education institution is able to fulfil its obligations under the law, it will therefore be necessary to determine and record who, or which positions, are responsible for this within the institution. The following section lists the officers/positions involved.

5.2 Officers involved

Because higher education institutions are all different, they do not have the same organisational structures and roles. It is therefore up to the institution to identify which of its officers are or should be involved in the use of education data. Nevertheless, this Reference Framework specifies a number of positions that should almost certainly be included when establishing and recording responsibilities.

5.2.1 End users

First of all, end users are an important category of roles that needs to be looked at. Consider the following persons who may use education data for a specific purpose:

- Member of the Executive Board (e.g. to gain insight into key figures of enrolments and graduations)
- Education Director or Director of Education (e.g. to formulate policy on progression and study success)
- Policy officer (e.g. to provide substantiated policy advice)
- Lecturer (e.g. to gain insight into developments in the quality of their professional field)
- Support officer (e.g. to support lecturers in organising their digital education)
- Researcher (e.g. to conduct longitudinal research on the impact of a policy measure on study behaviour)
- Programme Director (e.g. to gain insight into recent trends and expectations for the future)
- Student (e.g. to get a better understanding of their own development in relation to their year-mates)
- Student counsellor (e.g. to better determine where or when a student needs counselling)

In most cases the end user will determine which data is used as education data, for what purpose education data is used and in what way. The end user is therefore the person who must ensure that education data is used responsibly. To help end users with this, an institution may for example make it compulsory to complete a privacy checklist before education data can be used. This checklist compels the end user to think carefully about privacy and ethics related aspects.

5.2.2 Data Protection Officer

Higher education institutions are obliged to appoint a Data Protection Officer (DPO).[11] The DPO's duties are internal supervision of compliance with laws and regulations in the area of personal data protection and providing advice on the obligations arising from the GDPR and the UAVG.

To guarantee that the DPO can carry out their duties adequately, they have an independent position. This means that the DPO may not receive instructions on how to carry out their work. The institution must also ensure that the DPO has sufficient resources to carry out their duties and that they are assisted by the institution in performing these duties. To avoid the situation where the DPO is like a 'butcher inspecting his own meat', the DPO does not take decisions on the processing of personal data within the institution.

The DPO therefore has no direct responsibility for the processing of personal data but does have a responsibility to give advice – on their own initiative or on request – about the processing of personal data and to supervise the processing of personal data in terms of compliance with legislation and regulations. Furthermore, the DPO can also play a monitoring role if they encounter situations in which the rules are not or not fully complied with, either intentionally or unintentionally.

The DPO's role is therefore mainly advisory and supervisory and they report to the highest management body, which will usually be a member of the Executive Board and, if necessary, the Supervisory Board. The DPO is also the contact point for the national supervisory authority and the Personal Data Authority. Moreover, data subjects should always be able to contact the DPO.

[11] A DPO must be appointed pursuant to Article 37 of the GDPR if the data controller is a public authority or body, if the data controller is primarily responsible for processing operations which, by virtue of their nature and scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale, or if the data controller is primarily responsible for processing special personal data on a large scale.

5.2.3 Privacy officer (privacy lawyer, privacy contact)

Many institutions will have a designated privacy officer in their departments and faculties who can assist colleagues in that department or faculty with questions about personal data processing or privacy. Since this position is vested in the department or faculty, the officer knows the subject matter their colleagues are working with and can, in many cases, provide practical assistance on specific privacy questions.

In addition to a privacy officer in the department or faculty, there will often also be a central privacy officer or team, for example a central privacy office or one or more privacy lawyers. These officers can be involved in more complex or cross-departmental or cross-faculty privacy issues. Again, it is up to the institution to decide whether to assign a particular responsibility to this central privacy officer or lawyer.

Privacy officers should not become a mere 'obligatory counter' for obtaining a stamp to proceed with the use of education data. The added value of these officers is that they can advise and support the end user and other parties in the institution in making the right decisions regarding the use of education data.

5.2.4 Medical Ethics Review Board

When the Dutch Medical Research Involving Human Subjects Act (WMO) came into force, it became mandatory for research involving human subjects to be approved by a recognised medical ethics review board (MERB). Most institutions with an academic medical centre have a recognised MERB. This body must approve any research that is subject to the WMO. When medical research not subject to the WMO requirement is conducted, it may be that approval from the MERB is required nonetheless, or that the MERB issues a statement to the effect that the research is indeed not subject to the WMO requirement. In practice, the use of education data will not generally fall under medical research. However, when education data is used for academic research, it cannot be ruled out beforehand that this may, under certain circumstances, be regarded as medical research. This is why the MERB is mentioned in this Reference Framework.

Perhaps more relevant here is the trend in recent years for institutions to set up non-statutory or recognised ethics review boards. This can be done by the institution as a whole or by non-medical faculties within an institution. This often happens in faculties that work a lot with personal data or with human test subjects, for example in economic or social sciences. Researchers at the institution or faculty concerned must, in that case, submit the research proposals to this ethics review board for advice or approval.

Again, such ethics review boards are set up to review a proposal to conduct academic research. Therefore, when education data is used for academic research, this research may need to be approved by an ethics review board.

Case study: Ethics Review Board

It may be beneficial to the responsible use of education data if researchers who wish to conduct academic research using education data are required to submit their research proposal to an Ethics Review Board. This can be either a faculty board or a cross-faculty board. Make sure there is sufficient privacy expertise in this Ethics Review Board.

Five faculties at the University of Amsterdam, for example, have an Ethics Review Board to which research proposals must be submitted if certain criteria are met.

Erasmus University Rotterdam has set up a Privacy and Ethics Board which assesses proposals for pilots and projects with education data and monitors their progress. This Board includes a member of the Ethics Board, a student, a lecturer, a researcher, a policy officer, a data scientist and the DPO.

5.2.5 The education data team

Often there will be an officer or team within an institution that provides for the use of education data. This can be done in various ways, for example by preparing the data and structuring it so that it can be used for analyses.

This officer or team must also ensure that the system works properly, for example by building and managing the required tools (technical or otherwise). This includes ensuring that the source files can be accessed in a secure and reliable manner.

In addition, the officer or team will often carry out requests for the use of education data from end users. They can specify the conditions under which an end user can use education data and ensure that these conditions are met.

5.2.6 Information Security Officer/Chief Information Security Officer (ISO/CISO)

The ISO or CISO supports an organisation in the field of information security and has knowledge of the possible technical and organisational security measures that can be

taken. However, the ISO/CISO is not responsible for taking the necessary measures; this is up to the officers who decide on the use of certain data or certain systems.

However, the ISO/CISO can help to make the right connection between threats and risks and to identify any management and security measures that are appropriate in a specific situation. However, it is up to the responsible officer to take (or not to take) such measures within their specific context.[12]

Finally, the ISO/CISO contributes to increasing information awareness among employees, whether or not in cooperation with other officers, such as the DPO.

5.3 Method of defining and recording responsibilities

As noted at the beginning of this chapter, apart from the obligation to appoint a DPO and set out their tasks and role, there is no further regulation on how institutions should organise the internal division of responsibilities. However, in order to use education data lawfully and carefully, and therefore responsibly, it is important that this division of responsibilities is made and recorded.

A 'normal' policy document can of course be used for this. This document sets out the tasks and responsibilities of the various officers involved in the use of education data in the institution.

Another way this can be done is by creating an RA(S)CI matrix. This lists the officers involved and makes it clear whether they are **R**esponsible, **A**ccountable, **S**upporting, should be **C**onsulted or Informed for a certain processing operation.

[12] Handreiking IB profiel CISO van de VNG.

RACI matrix

The European Data Protection Supervisor (EDPS) has included a basic RACI matrix in its guidelines on accountability on the ground.

	Responsible	Accountable	Consulted	Informed
Top Management		●		
Business owner	●			
DPO			●	
IT department			●	
Processors, where relevant			●	

Bron: Accountability on the ground Part 1 of the EDPS

6 Transparency and Accountability

The common thread in all previous chapters as well as in the GDPR and the UAVG and other codes of conduct and standards frameworks is transparency and accountability. Transparency contributes to trust in how an institution deals with education data, gives legitimacy to the use of education data by institutions and helps staff and researchers to make the right choices. Chapter 2 covered the principles of transparency and accountability.

In this chapter, the more practical side of the transparency and accountability requirement is addressed. Although the GDPR specifies what information must be communicated and when, it does not specify how this must be done. This Reference Framework therefore addresses the issue of what institutions should provide information about as well as when it is most appropriate to do so in the context of education data, and how best to do so. Finally, practical guidance is given on how an institution can be accountable.

6.1 What to communicate

An institution must first make it known that it uses education data in a way that is clear to everyone. This can be achieved in various ways, for example by making it clear to students and prospective students during enrolment that the institution uses education data. This can be done, for example, by mentioning it on the landing page on the intranet or website or by regularly sending all students an email about it. It is crucial that the information is given in a place and in a way that students will be able to find and read it.

Incidentally, it is not necessarily – and often not possible – to provide all the information about the institution's use of education data at that time. Therefore, a layered way of informing can be used, where the most important matters are mentioned directly and the further information can easily be consulted via a link to another page or a privacy statement.[13] In paragraaf 6.3. wordt nader ingegaan op het gelaagd geven van informatie.

If an institution intends to use education data, other information about its use must also be provided. The three-pronged approach – Purpose, Basis, Due Care – set out in Chapter 5 also provides the tools to provide the information in a structured manner.

[13] See also the Guidelines on Transparency of the Article 29 Working Group, last revised and adopted on 11 April 2018, starting on page 22.

6.1.1 Purpose

Under the GDPR, an institution must provide clarity on the purposes for which education data is used. As stated in Chapter 4, it is important to formulate the purposes for which data are used as precisely and specifically as possible. However, it will often not be possible to indicate beforehand for which specific purposes education data will be used. One way of solving this is to provide information in a layered manner. This means that at a higher level, information can be provided in general terms on the use of education data. The institution may, for example, indicate that it has decided to use education data only to gain general insights for the improvement of education or education policy, or that it will only be used for individual guidance of students.

At a lower level, more details should then be given on the specific purpose of a particular use of education data. For example, if a lecturer intends to use education data for his own course to gain insight into the results over time of the students or the number of students who have followed his course, he must be transparent about this. The layering of information is discussed in more detail in 6.3.

6.1.2 Basis

In addition to the purpose, the legal basis applicable to the processing of personal data must also be communicated. Here, too, it is possible to communicate the basis for data processing in a layered manner. At a higher level, it can then be indicated which bases might be used for certain applications of education data. At a lower level, it can then be communicated which basis is actually used for a specific application, for example, that an institution has a policy that individual interventions can only take place on the basis of consent.

If the legal basis is 'legitimate interest', the weighing of interests carried out in this context should also be communicated.

6.1.3 Due care

In addition to purpose and basis, all other considerations must be communicated to ensure that education data is used responsibly and properly. Some of these are specifically mentioned in the GDPR as elements on which information must be provided. This concerns information about:

- What personal data is used;
- Identity and contact details of the data controller;
- Whether the personal data is shared with one or more other organisations and if so, which type of organisations;
- Whether the personal data is transferred to a country outside the European Economic Area or an international organisation and, if so, what guarantees are in place to ensure that this is done in a lawful manner;
- How long the personal data will be kept and, if this is not possible, at least the criteria for determining the retention period;
- That the data subject has certain rights (see also Chapter 7);
- That the data subject may always withdraw consent, if consent has been the legal basis according to which the data is used; and
- Whether it is a legal or contractual obligation for the data subject to provide the data and the consequences of not doing so;
- Whether there is any automated decision-making and if so, useful information about the underlying rationale and the expected consequences (see 7.8);
- If data from another source/processor are used, what the source is;
- The contact details of the DPO; and
- That the data subject may lodge a complaint with the institution itself or with the Personal Data Authority.

Higher education institutions usually have this information recorded in a general or specific privacy statement.

6.2 When to communicate

The premise is that this information must be given at the time of data collection. Since education data will almost always involve personal data that was originally collected for a different purpose, information about the use of education data will have to be provided in general terms wherever the data is collected directly from the data subject (see also 6.1.). However, this is not sufficient to meet all transparency requirements.

This is why it is best to communicate the specific use of education data at the time when the data will actually be used as education data. In practice, this will often be after determining the specific purpose for which education data will be used, what the basis is, what data will be used for this, how the data will be used and what measures will be taken.

If the information cannot be given at the time of analysis, it must in any case be given within a reasonable time, but no later than one month, after the data will be used as education data.

Case study: information obligation

A policy officer of an institution's Law Faculty wants to know whether there is a difference in the numerical results of a course taught in English and in Dutch. He would like to include the figures of all students taking or who took this course in the past two years, which is a total of around 2,000 students. He does not need or use any other information about the students.

Even in the case of a less invasive application of education data such as this, the information obligation must be met. As a minimum, this possible use should be included in a general privacy statement.

If the use of education data leads to direct contact with the person concerned, for example in the case of individual interventions for the study success of a student, information about the fact that education data is being used must be provided no later than at the time of contact.

Case study: student counselling

A student counsellor sees that a student has requested a meeting with her because the student is having problems with their studies. In order to prepare for the meeting properly, the counsellor uses education data to gain insight into the student's development. She not only uses data about grades and credits, but also information about the student's study behaviour, such as when they are most active in the LMS.

The counsellor will have to inform the student at the start of the interview that she has also requested information other than grades and credits. In view of the rights of the student – who is the data subject – (see also Chapter 7), the student must also be given the opportunity to respond..

And finally, if the transfer of education data to another institution or organisation is being considered and the data subject or data subjects have not yet been informed, this must be done at that time.

Case study: data sharing

Another institution asks University of Applied Sciences X for education data on the number of students enrolling from secondary school with a profile in Economics & Society, and is considering whether to supply this data to the institution.

If it concerns traceable education data, University of Applied Sciences X must inform the students concerned in advance. Depending on how many students and what kind of education data is involved, this can be done by sending a general email to these students or by placing a general message on the faculty web page, intranet or newsletter.

6.2.1 Exceptions

It is not necessary to provide the information if the institution has already informed the data subject, if receiving or providing the data is explicitly prescribed by European or Dutch law, or if the personal data must remain confidential on the grounds of professional secrecy or legal obligation of secrecy.

Moreover, the information mentioned in 6.1. does not have to be provided if it proves impossible or would require a disproportionate effort, especially if the further processing is for historical or academic research purposes, or if achievement of the purposes becomes impossible or is seriously jeopardised as a result. This exception must be interpreted strictly, however. It means, for example, that if email addresses are known it is no longer impossible or no longer requires a disproportionate effort to inform the data subjects. Furthermore, appropriate measures must be taken to protect the rights and interests of the data subjects.

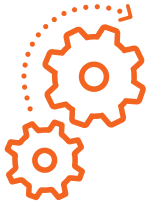
6.3 How to communicate

As indicated several times in this chapter, not all information needs to be given at once. This may also be done in a layered manner, for example by providing very general information at the time the data is collected from the data subjects, such as during enrolment. It is also a good idea to make such general information available to data subjects at all times, for example on the landing page of the website or the intranet. If necessary, an annual mailing can be sent out with the most relevant information.

The general notification can then refer to a general privacy statement, which contains further information on how personal data is used by the institution. Part of such a privacy statement can be devoted to the use of education data.

In addition to a general privacy statement, another option is to draft a privacy statement specifically for the use of education data by the institution. This could set out the choices and considerations for which education data can and may be used within the institution.

Finally, the considerations regarding a specific use of education data and all relevant information in that context can be published, for example by making a web page available per faculty or department or by providing the required information on the website of the relevant research project.



Case study: education data dashboard
Communicate as proactively as possible, for example through an education data dashboard, which education data is used for which types of applications of education data.

6.4 Register of processing operations

Under the GDPR, all institutions are required to keep a register of the personal data processing operations carried out by their organisation. This register need not be made public, but must be available on request to the DPO and the national supervisory authority. The following information must at least be included in this register:

- The name and contact details of the organisation and of the DPO
- Per processing operation:
  - The processing purpose
  - A description of the categories of personal data and the categories of data subjects
  - The categories of recipients and/or the personal data that will be provided to recipients outside the EU (in that case, also the safeguards that have been put in place for the protection of the data)
  - The retention periods (if possible)
  - The technical and organisational security measures

There is no procedural requirement for the Register of Processing Operations. For small organisations, an Excel file may be a solution, while larger organisations may benefit more from an online system.

The processing of personal data within the context of using education data will also need to be included in the Register of Processing Operations. The institution will therefore have to make it possible for the processing operation to be entered in the register. The best way to do this will vary from one institution to another, as it will also depend on who is responsible internally and how the register is kept.

Example: Register of Processing Operations
The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*; AP) has published its Register of Processing Operations on its website: www.autoriteitpersoonsgegevens.nl.

6.5 Accountability

As explained in Chapter 2, accountability means taking responsibility. An institution can do this by carefully weighing up conflicting interests or principles and also by making clear who within the organisation is responsible and accountable for this. An institution also does this by taking account of the fact that education data is always used in a certain societal context.

Institutions can do this both top-down and bottom-up:

- Top-down: institutions establish clear processes regarding the use of education data and demonstrably act in accordance with these processes. This ensures accountability for the decisions that have been made.
  - The first consideration that institutions must make is whether a particular purpose is in line with the institution's core values and its role in society.
  - Furthermore, institutions should document – on behalf of the data subjects – what is done with which education data and for what reason.
  - It should be possible to explain these considerations and they must be accessible to data subjects.
  - Institutions must continually assess whether the intended purpose has been achieved and whether any changes are necessary (Plan – Do – Check – Act cycle).

- Bottom-up: all data subjects must be able to count on the professionalism of the staff members who work with education data. These employees take responsibility for their actions and are accountable for it. If necessary, they also call others to account.
  - The ethical as well as the legal considerations are part of daily practice for everyone who works with education data. After all, it concerns day-to-day decisions in the workplace, where the question of what is ethically and legally responsible must be continually asked and discussed.

- Institutions can promote this daily practice by making the discussion about privacy and ethics part of their day-to-day work. It is important that staff who work with education data do not experience unnecessary external pressure through competition, work pressure, hierarchy or regulation.
- Where possible and relevant, institutions should apply a participatory process by involving students and other data subjects in the development and decision-making process, for example when introducing new techniques or applications for the use of education data.

7 Rights of data subjects

As explained in Chapter 4, in the case of education data the data subjects are students, prospective students, interested parties, former students, lecturers, counsellors and all other persons whose personal data is processed by higher education institutions. These data subjects have various rights in respect of their personal data. Institutions must provide for this, also with regard to the use of education data.

The various rights of data subjects are set out below and an explanation is given of how these rights can be incorporated within the framework of this Reference Framework.

7.1 General

Organisations are obliged to facilitate the exercise of rights by data subjects. This means that the institution may not create any unnecessary barriers for data subjects to exercise their rights and may not make this unnecessarily difficult.

In addition, the institution must provide all information in understandable language and in an easily accessible manner. A response must be given within one month of receiving a request for the exercising of one of the rights of data subjects. The deadline may be extended by a maximum of another month if the complexity of the request makes this necessary. In that case, information must be provided within the first month.

There is no legal requirement as to how the rights should be exercised by data subjects, nor how organisations must facilitate the exercise of these rights. It is up to each institution to give further substance to this in an appropriate manner.

In this Reference Framework

One example of how data subjects can exercise their rights is through a self-service portal. Through this portal, data subjects can inspect the information an institution holds about them to a certain extent (right of access), data can be amended, for example a change of address or telephone or account number (right to rectification), and possibly also irrelevant data can be deleted (right to erasure). For students and staff of an institution, this will often already be provided for in one way or another.

However, a self-service portal will not always be sufficient to provide information about all the personal data that an institution has and all the processing operations an institution carries out, including their use as education data. Nor is it necessarily accessible to all data

subjects, for example former students or other persons such as guest lecturers whose personal data is also processed and used as education data. It is therefore often necessary to make additional provisions to meet the requirement of facilitating the exercise of the rights of data subjects, for example by setting up a web form through which data subjects can submit their questions or requests or by providing an email address to which requests can be sent.

The provision of a web form or a specific email address to which requests can be sent is a way of facilitating the rights of data subjects. A request may, however, always be made and received in another way. Even in those cases, it will have to be considered as a request for the exercise of rights and answered in accordance with the applicable rules.

7.2 Right of access

Data subjects are entitled to know if personal data relating to them is being processed and, if so, to have access to that personal data. Case law shows that the main purpose of the right of access is to find out what personal data about a person is being processed and to verify the lawfulness of that processing.

There is also a right to obtain a copy of the personal data. It is important to note here that it is not necessarily a right to copies of the relevant documents, but of the personal data. If the rights and freedoms of third parties are affected when a copy of a document is provided, it is not necessary to provide it and such information may be omitted. The data subject may also be asked to specify their request.

In this Reference Framework

The right of access will generally be handled by a designated officer within the institution. This may be a privacy lawyer or another privacy officer within an institution, department or faculty, although, a request of access can be submitted at any place and in any form. If the request to access personal data is received by an officer who is involved in the use of education data, it is important to first coordinate with the officer who normally handles access requests.

An institution may decide to ask the data subject whether the request is for all data held by the institution or whether it is limited to the personal data relating to the specific use of education data. If someone asks for access of the use of their data for education data, the relevant information must be provided. Where education data is used for individual interventions in particular, or in any case for non-general applications, access must be given to the personal data used for the specific applications.

7.3 Right to rectification

In addition to the obligation for organisations to ensure that the data they use is correct (see 4.3.), data subjects have the right to seek rectification of their data. This means that they can request correction of incorrect data. This is not an absolute right; it may be verified that the correction is indeed a rectification. Where appropriate, this right may also be exercised by including an additional statement. The latter is relevant particularly where subjective assessments about a person are concerned and the assessor considers the original assessment correct but the data subject has a different opinion.

In this Reference Framework

The data used as education data will almost all have been originally collected by the institution for a different purpose. Any correction of incorrect data will therefore often have to be made in the source files. As far as subjective data is concerned, when using education data it is important to bear in mind that the right to rectification may also be exercised.

7.4 Right to erasure

A data subject may request the erasure (deletion) of their personal data. However, this is not an absolute right. The right only applies in the situations prescribed by law, for example if the data is no longer needed, consent is withdrawn (if consent was the basis) or if the data was processed unlawfully, but also if someone has objected to the processing and the organisation has no overriding compelling legitimate grounds for using the data.

In this Reference Framework

The right to erasure applies separately to the use of data as education data. A data subject may, in principle, request erasure of their data from the set of data used for education data without also requesting erasure of their data from the source files. However, if both are requested, both requests should in principle be treated separately.

Case study: right to erasure

A student has discussed his learning disability with a student counsellor, but does not wish to have it officially recorded in the institution's system. It is not a problem for the student that this is mentioned in the report of the meeting with the student counsellor discussion, but as soon as he finds out that it is also known to a student counsellor through the use of education data, he can request its erasure.

Whether a request for erasure should be honoured, moreover, depends on the circumstances of the processing and the request. If consent was the basis for the processing of education data, the withdrawal of consent may result in the data having to be erased. If the basis is that it is necessary for a task in the public interest or for fulfilling the legitimate interest of the institution, it will have to be assessed whether there are no longer any overriding legitimate grounds for the institution to still use the data as education data. This assessment will have to be made on a case-by-case basis.

If education data is processed for the purpose of academic or historical research, a request for erasure may be refused if erasure would make it impossible or seriously jeopardise the realisation of the purposes of the processing.

7.5 Right to object

Data subjects have the right to object to the processing of their personal data. This must concern processing that is based on the basis that it is 'necessary for a task carried out in the public interest' or 'necessary for the legitimate interests of the institution'. A higher education institution must cease processing personal data unless it has compelling legitimate grounds that outweigh the interests, rights and liberties of the data subject or that are connected with the establishment, exercise or substantiation of a legal claim. In such cases, a higher education institution must make its own assessment.

In this Reference Framework

Given that most processing of education data will take place on one of the aforementioned bases, data subjects will be able to exercise their right to object. If a data subject objects to the use of their data as education data, the institution must comply with this request unless it considers that it has compelling legitimate interests to process the data nonetheless.

If education data is used for academic or historical research, the data subject also has the right to object and this must be complied with, unless it is necessary for a task in the public interest to process or continue to process the data anyway.

7.6 Right to restriction of processing

A data subject may request restriction of the processing of their personal data under certain circumstances. This is allowed if, for example:

- the accuracy of the data is disputed and the institution verifies this; or
- the processing was unlawful but the data subject does not want the data to be deleted; or
- the institution no longer needs the data but the data subject does not want the data to be deleted for legal reasons; or
- the data subject has objected and a review is carried out to determine whether the legitimate grounds of the institution take precedence.

In this Reference Framework

In practice, this right is very rarely exercised. However, if there is a restriction on the processing of data, for example because its accuracy is contested or it is being reviewed whether the data should be erased, it means that the data may not be further processed as education data. Therefore, if a data subject has exercised their right to restriction on the processing of data, the institution must ensure that this is also respected by no longer making the data available for education data purposes.

7.7 Right to data portability

A data subject is entitled to request that personal data an institution holds on them be put into a structured, commonly used and machine-readable form and that this data be transferred to another organisation, for example another institution, without barriers. Where possible, the data subject also has the right to ask the institution to transfer the data directly to another organisation.

A data subject may exercise this right only in respect of data processed on the basis of consent or when it is necessary for the performance of a contract and the processing is automated.

In this Reference Framework

In particular, when education data is used for individual interventions and the basis applied is consent, the data subject may exercise the right to data portability, for example by sharing the results with another institution or organisation.

7.8 Right to avoid automated decision-making

The right to avoid automated decision-making could also be interpreted as a duty of organisations not to make automated decisions, including profiling, if this decision has legal consequences or otherwise significantly affects the data subject. This means that analyses made of people or groups of people for the purpose of decision-making that may affect individuals may never be fully automated.

There are a number of exceptions to this prohibition, for example if the automated decision-making is necessary to conclude a contract (for example, when taking out a mortgage) or if the data subject has given explicit permission. In such cases, measures must be taken, such as the right to human intervention, the right for the data subject to express their point of view and the right to challenge a decision.

In this Reference Framework

If education data is to be used for decision-making and these decisions have legal effects on one or more individuals or affect them significantly in some other way, this should not be done in a fully automated way. At the very least, the institution will have to provide for the possibility of human intervention and the right of the data subject to express their point of view or challenge a decision.

Particularly with respect to monitoring or following students' progress, it is important that any legal consequences arising from this, or consequences that significantly affect the student in any other way, are not fully automated. Having a 'human in the loop' and human intervention are explained in more detail in 2.2.4. The human factor is important, both in the process of automation and in the possible consequences of automation.

7.8.1 Artificial Intelligence

The emergence of AI is a significant development that often comes up in the area of automated decision-making in particular, but which covers much more. AI is increasingly used to analyse data. There are various forms of AI, from relatively simple algorithms to very complex, self-learning algorithms.

Which form is the most appropriate will depend on the purpose for which the algorithm is used and what results it is intended to achieve.

If an institution uses AI when working with education data, regardless of how advanced the algorithm is, the institution remains responsible for the responsible use of education data. This means that all the obligations and requirements set out in this Reference Framework, among others, apply in full, including the three-pronged approach in Chapter 4.

First, the institution must determine why it is necessary to use the algorithm. Next, the purpose of processing by the algorithm should be determined and justified, as should the basis of the processing and how the requirements of due care are met. The obligation of transparency is also fully applicable. An institution must therefore, among other things, substantiate what data is used by the algorithm, what the algorithm does with it, what the expected results are and how the results will be used. As described in 6.1.3, the use of algorithms requires an understanding of the algorithm or at least useful information on its logic.

An important condition for the use of algorithms is furthermore that the algorithm is 'fair' and that it can therefore be explained and guaranteed that use of the algorithm will not lead to improper results. In concrete terms, this means that the design must be carefully thought through beforehand: is the chosen algorithm suitable for the purpose? Has the operation of the algorithm been sufficiently tested? Are the measures and safeguards appropriate? What would happen if the algorithms unintentionally produce the wrong result?[14]

Finally, as indicated in 7.8, the use of AI must never lead to automated decision-making, including profiling, that produces legal or other significant consequences for the data subjects. In any case, human intervention should always be ensured.

[14] See also the AP website: autoriteitpersoonsgegevens.nl/nl/nieuws/toezicht-op-algoritmes

8 Other safeguards and measures

The previous chapters dealt with the most essential preconditions to which an institution must pay sufficient attention when using education data, namely the institution's responsibilities, the internal division of responsibilities, the obligation of transparency, and the rights of data subjects.

In addition to these essential preconditions, there are a number of other safeguards and measures to which an institution must pay closer attention. These are:

- Data Protection Impact Assessments (DPIAs)
- Cooperation with other parties
- Security and Privacy by Design

8.1 Data Protection Impact Assessments

A DPIA is an assessment of the impact and risks to privacy, or rather data protection, associated with an intended use of data. Of course, it is always beneficial to make such an assessment, but in a number of cases, carrying out a DPIA is in fact mandatory. If a processing operation is likely to present a high risk to the data subject or data subjects, a DPIA must always be carried out.

To determine whether a processing operation is likely to present a high risk, the nature, scope, context and purposes of the processing should be taken into account. Fortunately, much more detail has already been given as to what is meant by 'high risk' and in which cases a DPIA must be carried out. According to the GDPR, a DPIA will always have to be carried out in the following cases:

- A systematic and extensive assessment of personal aspects of natural persons which is based on automated processing – including profiling – based on which decisions are made that have legal consequences or otherwise significantly affect the person (see also 7.8. in this context).
- If special personal data is processed on a large scale.
- If public areas are monitored systematically or on a large scale.

As a supplement to the above cases, the European privacy authorities have jointly drawn up a list of nine criteria for assessing whether there is a high risk. Think of criteria such as automated decision-making (which does not necessarily lead to a decision with legal consequences), special personal data (not necessarily on a large scale) and large-scale

processing (not necessarily of special personal data). If two of the nine criteria are met, it can be assumed that there is probably a high risk.[15]

Furthermore, all national supervisory authorities have drawn up their own lists of situations in which a DPIA should be carried out. The Dutch supervisory authority has drawn up a list of seventeen types of processing for which a DPIA must be carried out. This includes matters such as covert investigations, blacklisting, profiling and observation and influencing behaviour.[16]

A DPIA always consists of at least four parts. First, it contains a description of the intended processing operations, the purposes and if the basis is 'legitimate interest', also the interests of the organisation.

Next, an assessment must be made of the necessity and proportionality of the use of data in relation to the purpose. Third, a risk assessment must be made. Finally, the measures taken to guarantee the protection of personal data and to demonstrate that the legal requirements have been met must be specified.

In this Reference Framework

A DPIA will not be compulsory for all uses of education data. For each specific use of education data, it will therefore need to be determined whether an intended use of education data is likely to involve a high risk and therefore whether a DPIA is required. To help determine this, many institutions have developed a pre DPIA or privacy checklist which should be completed before starting a project or an education data application. The pre-DPIA or privacy checklist includes the criteria of the European supervisory authorities and the processing operation from the list of the Dutch Personal Data Authority (AP) in question form. By completing a pre-DPIA, it becomes clear whether or not a full DPIA must be carried out.

Tip!

Make sure that a pre-DPIA or privacy checklist has at least the same input fields as those to be included in the Register of Processing Operations (see 6.9). In this way, two requirements can be met simultaneously.

[15] See the EDPB Guidelines on Data Protection Impact Assessments (WP 248)

[16] The AP's list is set out in the 'Decision on list of personal data processing operations for which a data protection impact assessment (DPIA) is required, Authority for the Protection of Personal Data' in Netherlands Government Gazette No. 64418 of 27 November 2019.

As there are no formal requirements for a DPIA, it can be done in a way that best suits the institution, as long as the four points mentioned above are included. In practice, however, it is useful to introduce uniformity in how a DPIA is carried out within an institution. This helps those performing the DPIA to avoid having to reinvent the wheel and prevents a jumble of templates. It also provides certainty that all required aspects are included in the assessment. Finally, it gives the possibility to compare different DPIAs and to have someone, for example the DPO, check whether it is done correctly. If the institution has not yet developed its own DPIA template, there are many examples available that can be used.

In detail: DPIA

SURF has a DPIA template available on its website: www.surf.nl/algemene-verordening-gegevensbescherming-avg/impact-en-riskassessment?dst=n1478

It is up to the institution to decide who should complete the DPIA, also bearing in mind the division of responsibilities described in Chapter 4. It is usually the end user of education data who must do this, or who is in any case very closely involved. It is important, however, to involve multiple disciplines in thinking about and looking the DPIA so that all risks and measures are properly reviewed. In some cases it can also be beneficial to involve a technical expert, for example if a new technique is used or if the processing is to be done with algorithms or AI.

8.2 Cooperation with other parties

Cooperation between one or more organisations can take various forms. For example, one or more parties may jointly determine that they will use data for a certain purpose, as well as which data and how this will be done. In that case, we refer to these parties as joint data controllers (see also 3.4.3). The joint data controllers must make agreements about who bears which responsibilities within the cooperation. The essence of these agreements must be communicated openly to data subjects. It must also be clear where data subjects can turn if they have questions or wish to exercise their rights.

It may also be the case that an organisation hires another organisation, for example for the provision of an IT service, including the supplier of the LMS. This other party performs the work under the direction of the hiring organisation and does not decide itself what is to happen with the personal data. In this case, there is a processor relationship. In such cases, agreements must be made between the data controller and the processor on, among

other things, how the processor is to process the data, what duties it has towards the data controller and what should happen after processing is completed. To this end, a processing agreement is concluded.

Finally, cooperation can also take place between two data controllers without them acting as joint data controllers. Consider, for instance, an organisation that wishes to use a set of data from another organisation, while the latter has nothing to do with the actual processing. In that case, agreements can be made about the use of the data, but this is not mandatory.

In detail: Purpose – Basis – Due care in the exchange of data

For all processing operations, the three-pronged approach in Chapter 5 applies!

When providing data, a well-defined purpose, a legal basis and appropriate care measures must therefore be taken. This is also true for any receipt of data.

In an exchange between institution A and institution B, both institutions must have a purpose and a basis for both the provision and receipt of data. If this is lacking, the exchange is not permitted.

If an institution intends to collaborate with another party on the use of education data, it must determine what form the collaboration will take, as the right agreements will have to be made on this basis.

Many institutions will have their own templates for making agreements, such as a processing agreement or a joint accountability agreement, that must or can be used for this purpose. If agreements have to be made, it is highly recommended and perhaps mandatory for some institutions to involve a privacy lawyer.

In detail: processing agreement

SURF has a template processing agreement and a template for joint controllers available on its website: www.surf.nl/files/2019-04/SURF-Model-Verwerkersovereenkomst-3.0.pdf and www.surf.nl/files/2019-01/model-gezamenlijk-verantwoordelijke-novk-1.0.pdf.

Tip!

When collaborating with another organisation, make sure that the principles for the use of your own institution's education data are also endorsed and respected by the other organisation.

8.3 Security and Privacy by Design

As there is already a great deal of other material available on the subject, this Reference Framework only deals with data security to a limited extent. It is important to mention this, however, since it is also relevant from an ethics and privacy point of view to take appropriate technical and organisational security measures.

The general principle is that appropriate technological and organisational security measures must be taken, such as pseudonymising and encrypting data, guaranteeing the confidentiality, integrity, availability and resilience of the systems and regularly testing and evaluating the measures taken.

Attention should already be paid to the security measures to be taken when conceiving and developing new applications or technologies. This is called privacy by design. Furthermore, the standard settings of applications and systems should be set to be as privacy-friendly as possible. This is called privacy by default.

In detail: information security

SURF has a lot of information available on its website, including an information security policy: www.surf.nl/en/information-security

SURF also has information available on privacy by design and privacy by default: www.surf.nl/privacy-by-design-en-privacy-by-default

8.3.1 Pseudonymisation and anonymisation

The terms pseudonymisation and anonymisation are frequently used in the context of privacy and the protection of personal data. The main difference between these terms is that pseudonymous data is still personal data, whereas data is only anonymous if it cannot (or can no longer) be traced back to an individual, using reasonable means, by any party. Properly aggregated data, for instance, can be anonymous to third parties.

But removing a person's name or replacing it with a number does not, by definition, mean that the remaining data is anonymous, especially if a document still exists somewhere by means of which the number can be traced back to a name. Even if such a document does not exist, there is a good chance that the remaining data, whether or not in combination with other information or documents, can be traced back directly or indirectly to a person. In academic education research, therefore – but also in other forms of use of education data – pseudonymous data is therefore more likely to be used than completely anonymous data.

So even if personal data has been pseudonymised, it is still personal data and the applicable rules must be observed. That said, pseudonymisation is a so-called Privacy Enhancing Technique (PET). It therefore has added value in the context of securing personal data. The risk for data subjects if something goes wrong, for example if the data falls into the wrong hands, is much smaller if the data is pseudonymised.

In detail: anonymisation and pseudonymisation according to the Dutch Personal Data Authority (AP)

The AP has paid a great deal of attention to the distinction between pseudonymisation and anonymisation.

In its recommendations to municipalities on the deployment of technologies in the context of smart cities, for instance, the AP has indicated that certain applications are – incorrectly – said to involve anonymised data. The AP emphasises that data can only be considered anonymous if it is unlikely for any party, using reasonable means (for the purpose), to identify individuals from it. The correct application of technology is also necessary to guarantee anonymity.

9 In closing

This Reference Framework contains the most important ethical principles and legal privacy frameworks institutions should take into consideration in order to use education data responsibly. In summary, higher education institutions should observe the following four ethical principles when using education data:

1. Institutions are accountable for and transparent about the use of education data and they account for it.
2. Whenever using education data, institutions must balance the interests of all stakeholders and data subjects in a fair manner.
3. Institutions should ensure that the analyses are reliable and valid.
4. There is always room for the human factor, even where institutions use automatic processes.

In addition, higher education institutions should pay specific attention to these four legal privacy elements when using education data:

1. The internal division of responsibilities is sufficiently well-defined and established.
2. The use of education data is communicated in a sufficiently transparent way.
3. Data subjects are supported in exercising their rights.
4. Institutions ensure that for each use of education data:
   a. The purpose is clearly defined; and
   b. The basis is clear; and
   c. The standards of due care can be properly observed.

9.1 Creation

In the preliminary stage, the Education Data Zone carried out an extensive survey into the question of whether there was a need for a national framework for the responsible use of education data. Talks were held with various parties involved, from various organisations at the administrative, policymaking but also executive levels.

This survey showed that the need for a national framework is widely shared. A number of preconditions were also specified, including that a national framework should mainly be directive and not prescriptive. This ensures that institutions that differ in terms of their nature, ambition, possibilities and wishes will be able to use education data in an appropriate manner.

In the spring of 2021, a so-called 0.8 version of the Reference Framework was created through collaboration with a large number of stakeholders. Seven experts from different organisations were closely involved in the authoring process, with a joint work session at the end of April 2021. In addition, a sounding board group of seventeen people was involved by interviewing some of them personally and informing them all in more detail during an information session in early May 2021. Both groups, as well as an even broader group of stakeholders, were sent a questionnaire with the request to reflect on the principles and the scope of the Reference Framework. Together, this resulted in the 0.8 version of the Reference Framework.

In the summer of 2021, a user group was established involving approximately twenty people from various institutions. This group started working with the Reference Framework in practice. In the autumn of 2021, an inspiration session was held with the user group for the purpose of identifying which points of the Reference Framework needed to be modified or expanded based on a discussion of case studies.

All this input was processed to prepare a 0.99 version, which was presented to members of the Executive Board during their meeting of 3 December 2021.

9.2 Future

This Reference Framework is a living document, which means that it has to be updated regularly to remain relevant and practicable. New technological, societal or practical developments may mean that elements in this Reference Framework will have to be adapted or that the Reference Framework will have to be expanded. The Education Data Zone of the Acceleration Plan will facilitate this process.

Credits

Project team
- Bram Enning (Education Data zone)
- Dominique Campman (Education Data zone)
- Dominique Hagenauw (D.E. Hagenauw)
- George Wurpel (MSG Strategies)
- Mariken Betsema (MSG Strategies))
- Niek Reijmers (MSG Strategies)

Focus group

Experts:
- Miek Krol (UvA)
- Martijn de Hamer (HvA)
- Tom Paffen (VU)
- Joyce Van der Klugt (HSL)
- Bart Karstens (Rathenau instituut)
- Theo Nelissen (Avans Hogeschool)
- Marit Van Ree (NRO)

Klankbordgroep:
- Reinout van Brakel (VSNU)
- Marcel Tillema (VH)
- Germaine Poot en Iris Huis in 't Veld (SURF)
- Leon Van der Neut (ISO)
- Susanne Rijken (IvhO)
- Frits Jacobs (LU)
- Leoniek Wijngaards (UU)
- Janneke Lommertzen (ResearchNed)
- Theo Bakker (De Haagse Hogeschool)
- Gert Douma (Hanze Hogeschool)
- Aramis Jean Pierre (DUO)
- Frederik Zuiderveen Borgesius (RU)
- Martine Baars en Jason Pridmore (EUR)
- Eline Terpstra (LSVb)

Gebruikersgroep:
- Marlon Domingus (EUR)
- Dominique Booms (HR)
- Bert-Jan Klaren (Hanze Hogeschool)
- Jesse Bruins (LU)
- Ineke Stoop (Tilburg University)
- Marjolein Blaauboer (VU)
- Jan Tjeerd Groenewoud (RUG)
- Lex Freund (HR)
- Marco van Leeuwen (BUas)
- Vera Heusschen (HSL)
- Roland Ettema (OU)

Special thanks to
Karen Maex (UvA) and Tineke Zweed (HU)
for contributing insights at the start
of this project.

The Acceleration Plan for Educational Innovation with ICT is a four-year programme set up by SURF, the Netherlands Association of Universities of Applied Sciences and the VSNU to bring together initiatives, knowledge and experience and to make rapid and concrete progress on opportunities for higher education. This takes place in eight different 'zones'. In the Education Data Zone, 11 institutions are involved in 16 sub-projects to make safe and reliable use of education data in higher education.

You can find more information and our publications at
www.versnellingsplan.nl