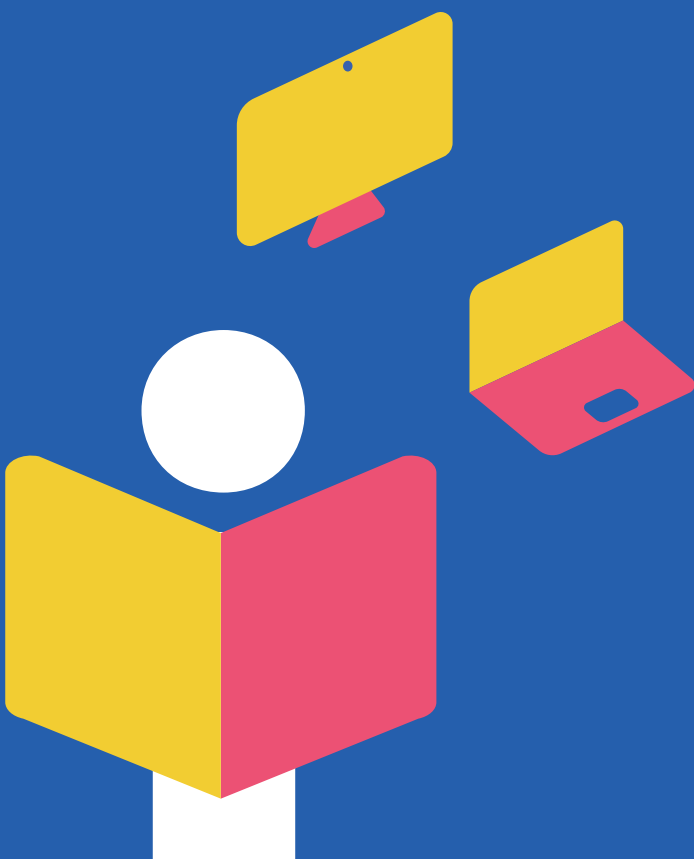


i-Learn PAPER 5

Data protection



Reference

 i-Learn team. (2022). *i-Learn paper 5: Data protection (5)*. i-Learn. URL

The i-Learn papers have been made possible by the complete i-Learn team, consisting of members of the imec, itec & KU Leuven consortium.

Published in June 2023.

Contents

Reference	2
About the i-Learn papers	6
Introduction	8
1. Digital data in education: the context	9
1.1 DIGITAL DATA ON THE RISE	9
1.2 DIGITAL DATA FOR EDUCATIONAL PRACTICE: A DOUBLE-EDGED SWORD?	10
1.2.1 THE BENEFITS OF DIGITAL DATA	10
1.2.2 THE PITFALLS OF DIGITAL DATA	11
1.3 DIGITAL DATA IN EDUCATIONAL PRACTICE: THE CHALLENGES	12
1.3.1 A LACK OF OVERVIEW AND AWARENESS	12
1.3.2 A NEW CHALLENGE FOR SCHOOLS	13
1.3.3 A NEW CHALLENGE FOR EDTECH PLAYERS	13
2. Ethical and legal preconditions for digital data in education: i-Learn best practices	15
2.1 BEST PRACTICE 1: KNOW THE RIGHTS OF DATA SUBJECTS	15
2.1.1 WHAT ARE THE RIGHTS OF THOSE WHOSE DATA IS PROCESSED?	16
2.2 BEST PRACTICE 2: KNOW YOUR DATA PROCESSING OBLIGATIONS	19
2.2.1 WHAT BASIC PRINCIPLES FOR DATA PROCESSING MUST ALL STAKEHOLDERS IN EDUCATION TAKE INTO ACCOUNT?	19
2.3 BEST PRACTICE 3: KNOW THE ORGANIZATIONS THAT HELP ENSURE PRIVACY RIGHTS	22
2.4 BEST PRACTICE 4: USE THE PROCESSOR AGREEMENT	24
2.5 BEST PRACTICE 5: IMPLEMENT A DATA POLICY	26
2.6 BEST PRACTICE 6: PERFORM A DPIA	27
2.7 BEST PRACTICE 7: STAY INFORMED	29
3. Conclusion	30
3.1 CHALLENGES AND RECOMMENDATIONS FOR EDUCATIONAL TOOLS	30
3.2 RECOMMENDATIONS FOR TEACHERS AND SCHOOLS	32

4.	Appendix 1: The DPIA for i-Learn	33
4.1	WHAT CAME WITHIN THE SCOPE OF I-LEARN'S DPIA?	33
4.2	WHAT WAS BEYOND THE SCOPE OF I-LEARN'S DPIA?	33
4.2.1	UNDERLYING PLATFORMS	34
4.2.2	RESEARCH BY ITEC	37
4.2.3	COACHING PLATFORM	37
4.2.4	SPECIFIC PROCESSING ACTIVITIES OF THE SCHOOL	37
4.3	THE PHASES OF I-LEARN'S DPIA	38
4.3.1	PHASE 1: WORKSHOPS	38
4.3.2	PHASE 2: DISCUSSIONS	38
4.3.3	PHASE 3: CONSULTATION WITH THE FLEMISH SUPERVISORY COMMITTEE	38
4.3.4	PHASE 4: LAST CHECK BY KU LEUVEN'S DPO	40
4.3.5	PHASE 5: PERMANENT FOLLOW-UP	40
4.4	RESULTS OF THE DPIA	40
4.5	CONCLUSION AFTER THE DPIA	42
	Sources	43

About the i-Learn papers

The i-Learn project was made possible by the Flemish government, KU Leuven and imec.

The i-Learn papers are the fruit of the eponymous project that was commissioned by the Flemish government in September 2019 and ran until June 2023. With the i-Learn project, the Flemish government aims to focus on the responsible and sustainable use of technology and help teachers to implement personalization in Flemish primary and secondary schools.

Through the i-Learn platform, we offer teachers and students accessible digital tools that do not alter the content of what students learn but rather the didactic framework. This supports daily classroom practice, in which the students and teachers are central.

By doing so, we give teachers more autonomy without increasing the burden of planning, and we give students insight into their learning process and the opportunity to participate in it. In addition, we are committed to the professionalization of teachers and the broadening of the Flemish EdTech sector.

The expertise and evidence-based practices that we have gained during the design, development and evaluation of the i-Learn project are now being recorded and disseminated through the i-Learn papers.



PURPOSE OF THIS PAPER

A lot of different data is needed to enable adaptability and personalization in learning platforms such as i-Learn. That data can be generated automatically through the interactions between the learner and the platform, the teacher and the platform, and through personal data that the learner or the teacher explicitly shares. It is very important to handle that huge amount of different data carefully, in order to ensure the privacy of the people who share it.

This paper aims to provide deeper insight into how i-Learn deals with the issue of data protection. In the first section, we outline the phenomenon of digital data in Flemish education. We also discuss the opportunities it affords, after which we comment on the evolution of this data. We examine the legal and ethical preconditions that tools must meet in order to handle data safely and responsibly. In the second section, we share six concrete tips on how to comply with these preconditions, based on our own practical experience at i-Learn. Finally, we conclude the paper with a call to come to the table with various educational partners and formulate clear, standardized guidelines for the entire sector. In that final section, we try to get the ball rolling by making four concrete recommendations, mainly aimed at policy makers and providers of educational tools.



In this paper, terms such as ‘digital technology’, ‘digital learning tool’, ‘online application’ and ‘tool’ are used interchangeably. These terms always mean: an online platform or app on which educational content is offered to students.

FOR WHOM?

This document has been compiled with the aim of sharing our knowledge of and insights into data protection in educational tools with a broad and interested audience. Each i-Learn paper provides an insight into the expertise, know-how and/or evidence-based practices that we have built up during the development and implementation of the i-Learn project.

In contrast to the previous papers, this paper focuses more on tool developers and suppliers, and on educational institutions. These parties have a great responsibility to ensure that the privacy of students, teachers and other educational actors is respected. That being said, this paper also offers very instructive insights for a wider audience, including teachers and school principals.

Introduction

In a 2022 report, Human Rights Watch revealed an alarming practice that did not reflect well on the educational technology sector. It claimed that no fewer than 146 of the 164 platforms surveyed worldwide had shared children's data with a third party, especially advertising companies that could approach the children with personalized advertising. Some of these platforms were also explicitly offered or recommended by national governments. A total of 39 governments were affected, including some from EU countries (Human Rights Watch).

The concrete findings were that learning platforms sometimes installed tracking technology on the learning platform without a disclaimer, that AdTech (*advertising technology*) companies sometimes gained access to students' unique identification data, and that the fundamental rights of the child were being tangibly undermined (Security.NL, 2022).

The problem of this trade in data, whether or not it is deliberate, first became clear during the coronavirus pandemic. When regular educational practice was upturned by the pandemic, schools and governments rushed to find ways to stay in touch with their students. The abrupt adjustment that resulted from that unprecedented situation meant that data protection was no longer a priority.

Though data trading or data leaks are not malicious in many cases, this state of affairs nonetheless raises a few important questions for Flanders. Could such data trading also come to light among Flemish tool providers? Is there a general binding framework that restricts such practices among educational partners for schools? Are schools sufficiently aware of the data about their students that is circulating?

1.

Digital data in education: the context

1.1 DIGITAL DATA ON THE RISE

Before we explore these questions, we want to start by outlining the context in which digital data is emerging in education. Over the past decade, the number of apps that use *digital data* have shot up. Today, marketers use data to tailor their ads precisely to you, government bodies rely on data to determine your earnings, benefits and taxes, and health institutions monitor your health based on the data in your medical record. This list of applications is far from exhaustive, and it is constantly expanding.

Of course, the education-technology sector has also embraced the benefits of data. More and more schools are striving to offer their students a personal learning experience so they can monitor their students' study pathways more closely. Various EdTech players have responded to this demand by launching apps that facilitate personalized learning. All these players have understood one thing: data has become indispensable in gaining a better understanding of the learning needs of students today, (De Argumentenfabriek & Het Kennisnet, 2016).

In particular, information belonging to students' private lives, their **personal data**, is valuable. This umbrella term includes all information that can be linked directly or indirectly to an individual. And what we mean by personal data is exactly what the name suggests: it's personal. Personal data may include surname, first name, age and gender, as well as educational or professional info such as the name of the school, the school year and the type of education.

Secondly, the EdTech field often focuses on **log data**. The processing of this data also greatly contributes to the creation of a personal learning environment. Log data means all technical information linked to an individual registration or login to a website, such as a username or password.

In recent decades, **learning analytics** (LA) has also entered the field. Through LA, data is generated from a student's activity, which allows the digital learning environment to be even more tailored to the student. The unique goals of learning analytics are understanding the learning process and optimising it in different ways.

The latter goal in particular has already received a lot of attention in the context of data in education. Students' individuality and the uniqueness of their learning processes are more important than ever. At the same time, it has become quite a challenge for teachers and school leaders to cope with learning diversity without support. That makes it unsurprising that quite a few tech companies see that there is money to be made in developing learning analytics.

LEARNING ANALYTICS IN I-LEARN

i-Learn also uses data to enable its learning platform and uses **Learning Analytics (LA)** for this purpose. In i-Learn, LA gives teachers an overview of their students' progress and learning processes by means of a dashboard system. In a test phase, LA was already used to give teachers new recommendations on learning tracks, based on their own activity.

Would you like to know more about Learning Analytics and what role they play for i-Learn? Please read Paper 3, which is entirely devoted to this topic.



Especially in the wake of the coronavirus pandemic, there has been significant growth in digitization and interest in digital data over the last few years. This growth has occurred in all sectors, including education. It is important to further stimulate the growth potential of LA and other tools. But at the same time, there are still a few growing pains to be healed: the EdTech market remains fragmented and various legal ambiguities remain (imec, 2022).

1.2 DIGITAL DATA FOR EDUCATIONAL PRACTICE: A DOUBLE-EDGED SWORD?

1.2.1 The benefits of digital data

Let us begin by considering the uses of digital data in education. There are already many applications available that focus on (1) supporting administrative tasks in education, (2) strengthening the teaching practice of teachers, and (3) improving the learning environment of students (Prinsloo, 2020; Selwyn, 2015). What interests us most in the context of this paper are apps that fall under categories (2) and (3). Those are what EdTech players prefer to focus on. Giving a complete overview of all possible educational applications would take us beyond the scope of this paper, so we are limiting ourselves to a small selection from the list of the benefits of digital data in the education sector:

1. First and foremost, data at an individual level can be used to personalize students' **learning** based on their interests, knowledge and skills. For example, smart tools can create a personalized learning environment for each student. They can also provide teachers with insight into their students' learning processes so that they can address each student's individual needs more effectively.
2. At the classroom level, data can also help teachers by enriching **teaching**. For example, a teacher can easily use data to group students with similar needs and thus provide further support to those that need it. Here, data improves efficiency for the teacher.
3. At both the individual and class levels, data can make **evaluation** easier. Learners can receive immediate feedback while doing exercises, and teachers can view a progress dashboard that allows them to interpret their learners' learning processes.
4. Finally, at the school or cross-school levels, data can be used to identify patterns and trends by comparing students' learning outcomes. Based on this, we can adapt our education policy or **develop** new study methods.

In short, the use of digital data can have a positive effect on (1) the learning process, (2) the teaching practice, (3) the evaluation practice, and (4) the further development of educational-pedagogical knowledge.

1.2.2 The pitfalls of digital data

Whether it is to increase the productivity of a teacher or to optimize learning outcomes, digital data can therefore strengthen the quality of education on various fronts. So it is better to embrace this innovation than to resist it.

However, as always with new technologies, there are also downsides. In practice, it appears that new players are still too lax about certain preconditions or restrictions before they start processing data. Yet the limitations we have created for ourselves are very valuable. They force us to think about the actions we take with the data (van Trigt, 2019).

Firstly, every data processor should fulfil a number of **didactic and technological preconditions**. These include the ability to analyse, interpret and relativize data properly. That seems logical, but a tool provider can only employ justified data analysis to facilitate the learning process if they have developed sufficient data literacy skills. The same applies to teachers, students and other educational support staff who incorporate data from a tool into the learning process.

But it does not stop there. Besides requiring data literacy, data processing the ability to reflect critically on ethical data handling. Furthermore, it requires some knowledge of the legislation.

We place these basic requirements for data processing in the category of **ethical and legal preconditions**. The principles of these preconditions are set down in the GDPR. That legislation requires schools and educational support institutions to properly document where, on what legal basis and for what purposes student data is processed. It also obliges them to protect the data.

THE GDPR

The General Data Protection Regulation (**GDPR**) is the European regulation that governs the handling of individuals' personal data (*Regulations: Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016*). The regulation came into force throughout the European Economic Area in 2018. It was formulated with the main aim of meeting the challenges that companies, governments and organizations face in processing personal data across national borders.

As the amount of data generated continues to increase, the conditions it sets out are becoming more important than ever. Data processing practices must be aligned with the EU's ethical and legal framework. Significant responsibility for this rests on the shoulders of tool providers.

1.3 DIGITAL DATA IN EDUCATIONAL PRACTICE: THE CHALLENGES

1.3.1 A lack of overview and awareness

Schools usually have a clear, complete overview of the data they use for administrative purposes. But when it comes to processing data in classroom educational applications, a clear overview is often lacking. Although some schools have developed or are developing a policy plan around digital learning resources, teachers often supplement their learning material with digital learning resources of their choosing. And these teachers are not always aware of where their students' data will go.

1.3.2 A new challenge for schools

At present, processing agreements are often concluded along with the contracts with the providers – we also call them **suppliers** – of such digital learning resources. Nevertheless, there are also many apps used by teachers in their teaching practice that do not require a contract, such as those from non-commercial providers or tools with free features. Awareness of data processing in these applications is often insufficiently encouraged or researched, so it leaves much to be desired. Several private companies have already responded to this lack by offering schools their expertise and services for a fee.

A more sustainable solution would, of course, be for companies in the EdTech sector to be able to comply with clear privacy regulations. In practice, however, there is still a great deal of uncertainty about the privacy regulations to be followed, as a result of which not all tools apply the same standards (Berghmans et al., 2020). Schools therefore have questions about working with certain tools and companies, and rightly so. Unfortunately, it can sometimes be difficult to find a more privacy-friendly alternative to certain services, and these privacy concerns can end up being swept aside.

1.3.3 A new challenge for EdTech players

At the same time, the GDPR brings a lot of new responsibilities for EdTech players. Given the responsibilities of schools, tool providers should consider it good business practice to provide optimal information to their school partners about the privacy policy they apply. However, the GDPR is a complex law full of rules and exceptions. So it can be difficult to see the proverbial wood for the trees. As a novice EdTech player, where can you find support?

We share our own best practices below and give some concrete tips to get the educational partners of schools started. We answer questions such as which students' rights tools should keep in mind, which principles the data processor must adhere to when using data, which authorities can provide an overview of the tangle of legislation and support with applying it, which documents are indispensable and how tools should work towards a watertight privacy policy.

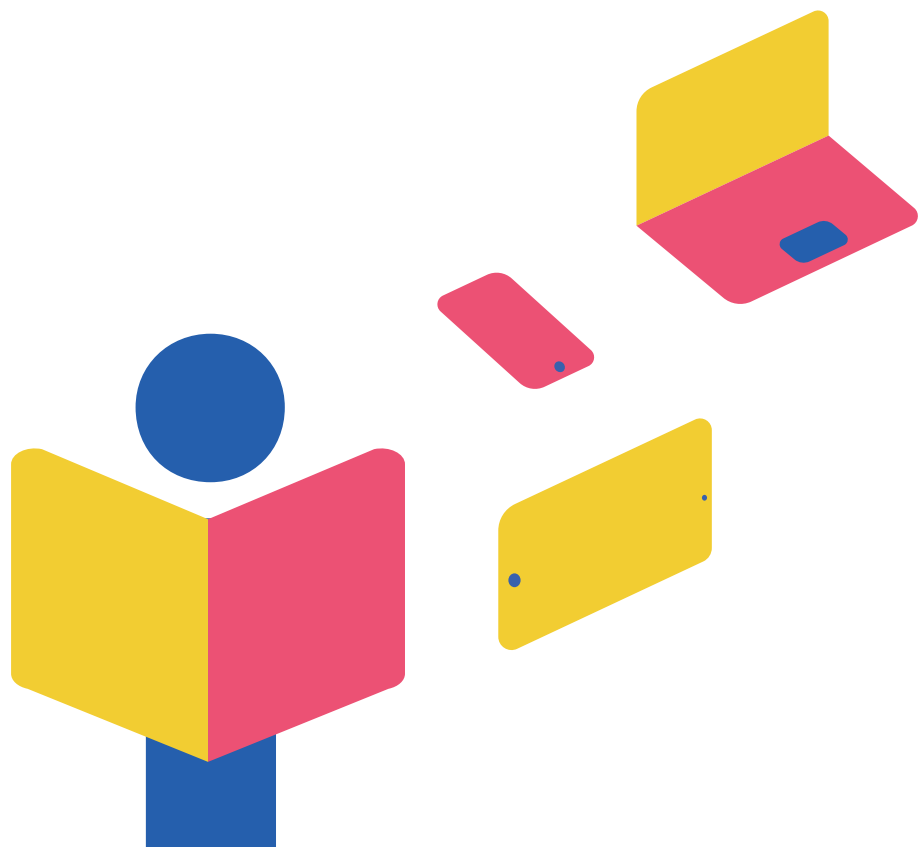


ESSENTIAL ROLES IN DATA PROCESSING

Data processing is a complex and structured process in which different players have strictly defined responsibilities. Two stakeholders play key roles in this: the data **controller** and the data **processor**.

- **The controller** is in charge of the data processing, and the party that is therefore also ultimately responsible for it. The controller determines the purpose, rules and means of the processing and may appoint a processor to support it.
- **The processor** processes the data on behalf of a controller. The processor cannot process or pass on personal data to third parties without the consent of the controller.

For our purposes, the controller is usually the school or educational institution, and the processor is usually the tool provider or supplier. However, it is important to realize that this division of roles may vary depending on the context of data processing ('De AVG in het onderwijs: dit moet je weten', 2019).



2.

Ethical and legal preconditions for digital data in education: i-Learn best practices

2.1 BEST PRACTICE 1: KNOW THE RIGHTS OF DATA SUBJECTS

When we think of data protection, the GDPR may be the first thing that comes to mind. The General Data Protection Regulation (**GDPR**) is the European regulation that governs the handling of individuals' personal data (*Regulations: Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016*).

A BRIEF HISTORY OF GDPR

A little background on the GDPR: before the law came into force in 2018, it had been in the pipeline for some time. The proliferation and circulation of data has raised many social, legal and ethical questions since the beginning of the 21st century. Moreover, the increasingly international context in which this data was circulating called for a harmonized policy within the European Economic Area (Burgess, 2020). National data protection laws were often inadequate to keep up with the evolving situation.

This is why the European Union issued the GDPR in 2016. Then it gave organizations and Member States two years to implement the new legislation. In Belgium, the GDPR finally came into force on 25 May 2018 and replaced its predecessor, the Privacy Act. Ironically, the need for this law had come to the fore a few months earlier. The Cambridge Analytica scandal, which revealed that the data company had obtained data from 87 million Facebook users (Jvh & Blg, 2022), was a textbook example of the consequences of privacy breaches.

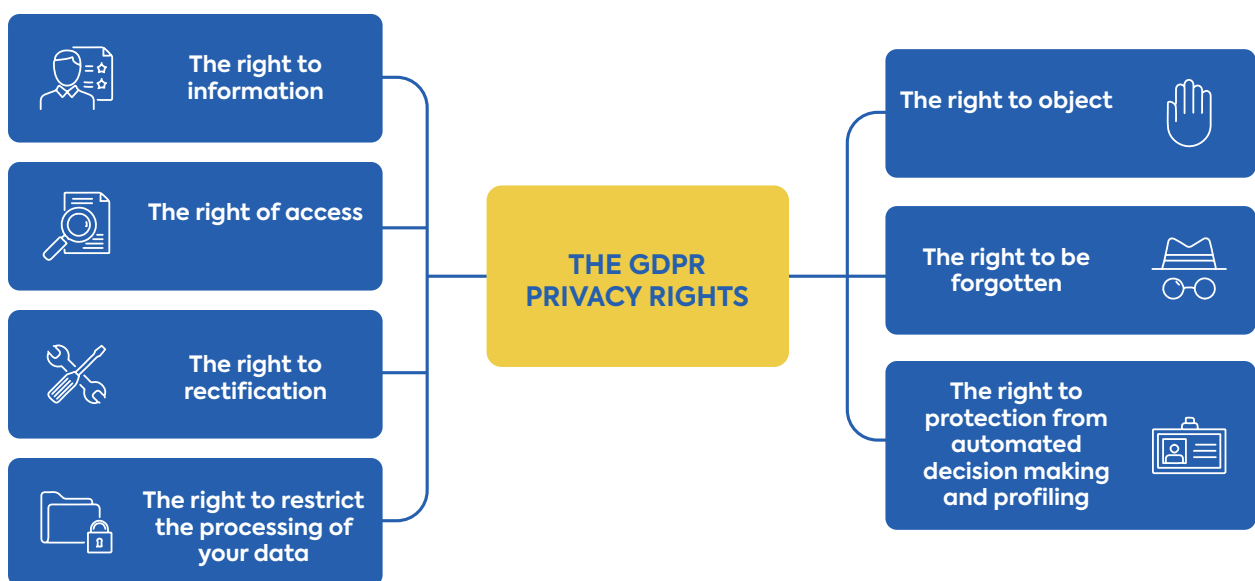
The GDPR provides a legal framework for the protection of all personal data within the European Economic Area (EEA). Clearly this includes personal data that comes from education. The GDPR states that schools, as data controllers, must be able to prove that they are correctly processing and securely storing the personal data of their students and teachers. This means that schools should only use tools that have a GDPR-compliant policy ('Wegwijs in de AVG voor Onderwijsinstellingen', 2018).

Hence our first recommendation for complying with the GDPR guidelines: **properly understand the rights of the person whose data you are processing, and know your obligations when processing personal data.**

2.1.1 What are the rights of those whose data is processed?

Each individual has a set of basic rights around which the GDPR is built. The data processor must take all these rights into account. The **data subject** – the person whose data is processed – has, among other things, the right to know who is processing which data about them, and for what purposes. The data subject must be informed correctly and in good time and, if necessary, provide free and informed consent to this processing. The data subject may withdraw their consent at any time, and it must be possible to correct the data. There are some other rights for data subjects, but these are not always absolute and can usually only be invoked in certain circumstances.

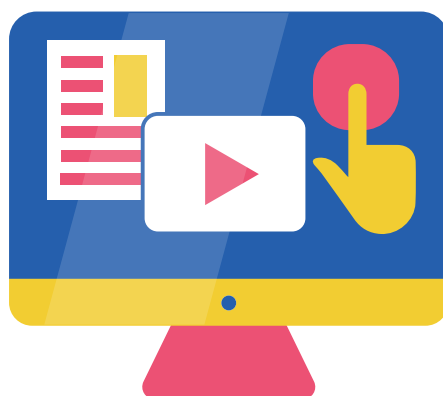
FIGURE 1: An individual's privacy rights as described in the GDPR



We will list the eight rights of the data subject, as set out by the GDPR, and give some examples of how they may be of interest to the processor. The controller is responsible for the correct application of these rights, but the processor has an important role to play as well.

1. The right to information: the data subject has the right to be informed of the data processing and all relevant related information. This right implies that the tool provider makes the efforts required to provide all necessary information in a clear and transparent manner. They can do this with an information brochure, for example, or a privacy statement on their website.
In order to comply with the right to information, the data subject must be informed about various matters, such as the retention period of the data and the procedures for objection, access and rectification. [Privacyinonderwijs.be](https://www.privacyinonderwijs.be) offers a more complete overview of this in its technical brochure 'WEGWIJS in de AVG voor Onderwijsinstellingen' (2018).
2. The right of access: the data subject must be able to view their processed data at any time or to request a copy of it. As an EdTech player, you can anticipate this right by devising a simple procedure allowing the educational institution to make the data available to the person concerned within a reasonable period of time.
3. The right to rectification: has the data subject exchanged incorrect or insufficient data, or has something changed in their situation? If so, the data subject must be able to easily correct the error or supplement the data. As a tool provider, it is best to have the necessary procedures to support the educational institution in this regard.
4. The right to data restriction: in certain situations, the data subject may choose to temporarily block the processing of their data. The educational institution must evaluate whether this request is justified and, if so, the tool provider must offer the opportunity for this right to be implemented, unless this entails an unreasonable effort or risk.
5. The right to object: in a number of cases, the data subject may object to the processing of their personal data. If so, the educational institution is responsible for balancing the interests of the data processing and the objection of the data subject. Depending on the legal grounds, the processing may then be stopped and the tool provider must comply with this. However, the right to object is not unconditional and can only be invoked in specific situations. That being said, there is one situation in which the right to object is always upheld: when personal data is used for marketing purposes.

6. The right to be forgotten: above and beyond objecting, a data subject may also invoke their right to be forgotten (right to erasure) in some situations. As this suggests, this means that the data subject can have all their data deleted. However, the right to be forgotten is not absolute either, because in many situations educational institutions have to process the data for legal or administrative reasons. If the data has to be deleted, the tool provider must also implement this correctly.
7. Right to data portability: A right that is less applicable to an EdTech player in relation to learners is the right to data portability. With this right, data subjects can request that the educational institution transfer their data in a digital and machine-readable format, so that it can then be reused for another service. Such requests for data portability are made, for example, when a student changes schools and wants to take their personal data with them. In this situation, the tool provider must support the educational institution in fulfilling this request.
8. The right to oppose automated decision making and profiling: this includes the right not to be profiled on the basis of your data. For example, if a tool uses algorithms that perform an automatic analysis – which in this case is equivalent to analyses without human intervention – on personal data, and thereby provides a student with profiling feedback or learning material, the student concerned can invoke this right. What is considered to be ‘profiling’ is set out clearly in the GDPR.

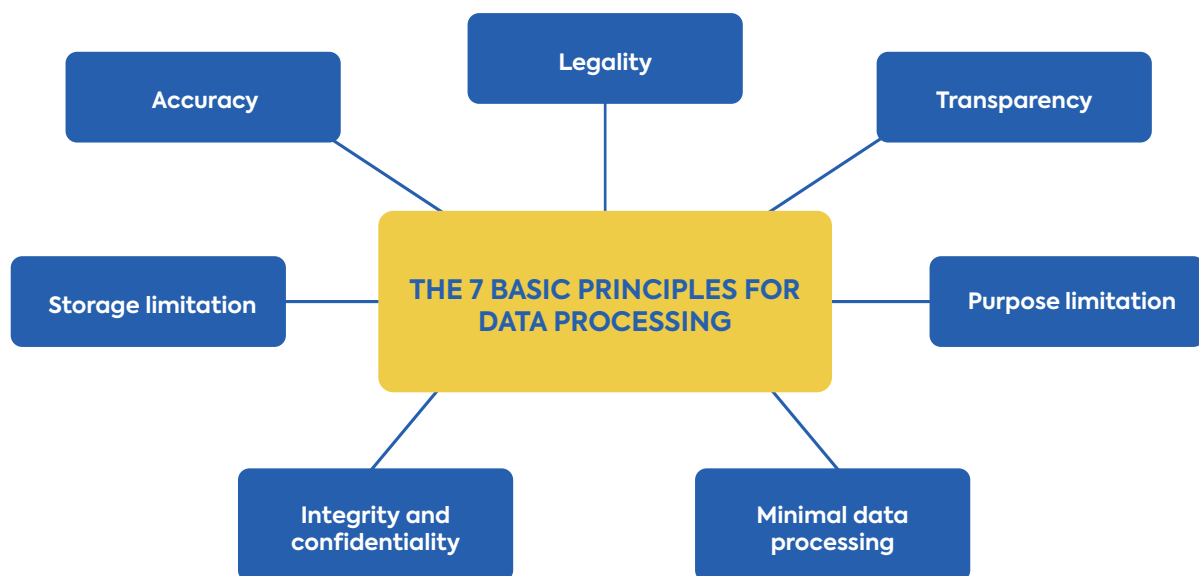


2.2 BEST PRACTICE 2: KNOW YOUR DATA PROCESSING OBLIGATIONS

2.2.1 What basic principles for data processing must all stakeholders in education take into account?

All stakeholders that process data should take a few limits into account, as stated in Article 5 of the GDPR. In the European legislation for education, there are nine key words for the processing of personal data that are usually bundled into **seven basic principles**: legality, transparency, purpose limitation, minimum data processing, accuracy, storage limitation and integrity.

FIGURE 2: The 7 basic principles for data processing



For all stakeholders within education, it is essential to use these seven principles as a compass to navigate the privacy landscape. We will therefore briefly consider these principles, to which every party that processes personal data for any form of data processing should adhere:

1. **Legality:** According to this principle, the processing of personal data must always be legally justifiable. In other words, it must be based on legal grounds ('Wegwijs in de AVG voor Onderwijsinstellingen', 2018). There are various legal grounds that frequently occur and are combined in education:

- a. **Legal obligations:** in some cases there is the possibility to rely on legislation to justify certain data processing. For example, on the basis of the Decree on the *Legal Status of Employees* of 27 March 1997, statutory data may be kept on employees for the smooth running of HR administration. These legal grounds can also be used for students, when teachers are required to keep attendance records.
- b. **The legal grounds of a contract:** student data may in some cases be kept on the basis of signed school regulations. This is called the legal grounds of a contract. Bear in mind, however, that the school regulations must provide optimal transparency about which personal data can be processed for which purposes, and the processing agreements that the school has made with various suppliers.



- c. **Legitimate interest:** schools and tool providers may also rely on legitimate interest for some processing of personal data for purposes such as security, evaluating possible improvements to apps and organising other necessary daily activities.

- d. **Public interest:** some schools might rely on public interest for certain processing activities because of their social obligations, such as the organization of education and associated activities.

- e. **Consent:** finally, the legal ground of consent is sometimes invoked in the school context, whereby the school requests explicit consent from a student and/or parents for the processing of personal data, such as the posting of a photo on the school website. It is important to note that data subjects must be able to withdraw that consent at any time, and that the school must be able to prove consent clearly and unambiguously.

- 2. **Transparency:** Avoid confusion and misunderstandings among the parties involved by always being open about what data is being processed and why. Transparency in terms of the GDPR means, among other things, that the informed consent process is active and complete. In addition, that information process must be clearly documented.

3. **Purpose limitation:** Purpose limitation means that a school may only use personal data for certain predetermined purposes, and not for others such as marketing or research. Objectives for which data processing can usually be justified without difficulty include student administration, student support and communication. If the school wants to process data for new purposes, it must set out new purpose limitations before it can start the new processing. Depending on what the new purpose is, it may have to be linked to another legal grounds from the GDPR (see legality above).
4. **Minimal data processing:** Another requirement that the GDPR prescribes is that no more data may be processed than is necessary and desirable. As a data processor, you must therefore conduct a reflection process in which you ask yourself what is ‘need to know’, and what is ‘nice to know’. Anything that is not relevant may not be included in the data processing without justification. For example, it may be interesting to know the profession of your students’ parents, but it can only be justified in specific cases.
5. **Accuracy:** processed data must also be correct and up to date at all times. This means, for instance, that a school must give students and parents the opportunity to have their own file corrected or updated if something is wrong. Taking appropriate measures to guarantee that accuracy is indispensable.
6. **Storage limitation:** A justifiable retention period must be established for each piece of data, so that it is not stored longer than necessary for the purpose. Those retention periods are usually set down in decrees. For example, the personal data of secondary school students is stored for five years after the completion of the secondary curriculum (Flemish Ministry of Education and Training, 2003).
7. **Integrity and confidentiality:** The GDPR also emphasizes that data must be processed within a technically secure and protected environment, with access limited to the teachers and school leaders for whom the data is of interest. It is up to the schools to take technical measures that ensure this, such as setting up two-factor authentication, installing a firewall on the school network and regularly performing system backups.

These seven fundamental principles of data processing – legality, transparency, purpose limitation, minimum data processing, accuracy, storage limitation and integrity – provide a solid foundation for responsible and ethical use of data. **Our second best practice guideline is therefore for tool providers to strive to ensure safety and trust for all those involved, by considering these principles to be of the utmost importance.**

2.3 BEST PRACTICE 3: KNOW THE ORGANIZATIONS THAT HELP ENSURE PRIVACY RIGHTS

Do you want to get started with data protection as a tool provider? Then it makes sense to find out which agencies can assist you in this. Because the truth is that not everyone can easily find their way round the maze of GDPR guidelines. Fortunately, there are specialized control and support bodies to assist compliance with a complex law such as the GDPR, including ones for education.

Let us start by looking at the control bodies. Firstly, the Belgian Data Protection Authority (DPA) acts as a watchdog for the basic principles of the GDPR. Their competence extends federally and across various sectors, both public and private. The tasks of the DPA are multi-faceted: they not only provide advice, but also focus on raising awareness about the GDPR. For example, the DPA launched the website ikbeslis.be to bring privacy to the attention of young people, parents and teachers. In addition, the authority intervenes in the event of data leaks and related violations. It is to the DPA that schools are first obliged to report such violations, after which its inspection service carefully maps out the risks and legal consequences of the situation.

Secondly, there is the Flemish Supervisory Commission (Vlaamse Toezichtscommissie, VTC), which monitors correct compliance with the GDPR within Flemish government institutions. The VTC was established in 2018, shortly after the GDPR came into force, and has the important task of advising the Flemish administrative authorities on the processing of personal data. However, it is important to note that, due to its focus on the public sector, the VTC does not control private companies.

The VTC is also responsible for education in Flanders, for which it regularly makes recommendations. An example of the influence of the VTC on education can be seen following the announcement of the Digital Leap (Digisprong). As part of the digitization plan, the Flemish government promised IT devices to every student. The VTC advised schools on how to deal with the purchase of this IT equipment and analysed the risks of large-scale purchases. For instance, it is recommended that schools pay sufficient attention to including privacy conditions in the technical specifications from their device suppliers (Digitaal Vlaanderen, undated).

THE DIGITAL LEAP (DIGISPRONG)

In Flanders, the implementation of digital data in education is emerging against the background of what is called the ‘Digisprong’ (‘Visienota Digisprong’, 2020). The Flemish government’s aims in developing this plan include the development of a targeted data policy, for example by creating a data-driven knowledge and advice centre. The plan explicitly states that data and artificial intelligence are necessary to shape the mission and policy of schools in the future. The policy plan also emphasizes the importance of following privacy regulations as a focal point for a data-driven school policy.

Finally, various **Flemish education providers** (i.e. all school umbrella organizations in the various education networks such as GO!, OVSG, POV and GVO) have set out guidelines for the practical implementation of the GDPR. They play a supporting role in protecting privacy. In a press release from 2018, shortly before the GDPR came into force, the education providers guaranteed that they had already taken some action to address privacy (*Press release: ‘Modelovereenkomst beschermt persoonsgegevens in onderwijs’*). For example, they had already raised awareness about privacy-sensitive information and designating contact persons for data security.

THE DECLARATION OF INTENT OF THE FLEMISH EDUCATION PROVIDERS

In the aforementioned press release of 2018, the education providers also announced a declaration of intent. When later issuing that declaration of intent, which was called ‘*Privacy in digitale onderwijsmiddelen*’ (‘Privacy in digital educational resources’), the school umbrella organizations, including major players such as KOV and GO!, committed themselves to actively support data protection in school communities. The declaration was signed by the majority of education providers as well as by other institutions such as the Vrije CLB-koepel (Free CLB umbrella), the Federatie Centra voor Basiseducatie (Federation of Centres for Primary Education), the Groep Educatieve en Wetenschappelijke Uitgevers (Educational and Scientific Publishers Group) and various software developers (‘*Intentieverklaring Privacy in Digitale Onderwijsmiddelen*’, 2018).

Incidentally, an important part of the declaration of intent was the introduction of a written contract, called a **processor agreement**. Schools could use this as a guide to protect themselves from risks when working with ‘data processors’. The agreement spells out the rules, in detail, for both the controller (e.g. a school) and the processor (e.g. a company that offers a digital educational application and must process student data for this purpose). More about the processor agreement can be found in the section on best practice 4.

From the VTC to the DPA and the Flemish education providers: the aforementioned control and support bodies provide valuable guidance and help tool providers navigate the complexity of the GDPR. **So our third best practice guideline for tool providers is to carefully align your policy with their advice and expertise.**

2.4 BEST PRACTICE 4: USE THE PROCESSOR AGREEMENT


In the previous best practice guideline, we mentioned that initiatives have already been taken by various parties to coordinate privacy and data protection in Flemish education. In response to the entry into force of the GDPR, those same parties (the VTC, the DPA and Flemish education providers) created an [exemplary guideline](#) in 2018 in the form of a **processor agreement** ('Model Verwerkersovereenkomst', 2018).

The processor agreement is a standard template that sets out the agreements between the various parties involved in data processing. It ensures that contracts between these parties have a clear and uniform character throughout Flanders. In addition, all mandatory legal and ethical provisions from the GDPR are reviewed. Many tool suppliers have since adopted the model.

What does the processor agreement consist of? The introductory part of the contract sets out some important agreements, including the division of roles in data processing, the purpose of the processing, the obligations of the processors and sub-processors, the rights of the data subjects and the consequences of breaching the agreement. This processor agreement is supported by two leaflets: a privacy leaflet, which explains the nature of the processing in detail, and a second leaflet, which provides an overview of technical and organizational security measures that processors must take if they share information or if a data leak occurs.

FIRST AID FOR DATA LEAKS

Despite all the preventive measures, what if you, as a tool supplier, still have to deal with a data leak? Article 7 of the processor agreement formulates the steps that the various parties must take to reduce the risk of a leak:

 Please note: not every data leak is considered risky. Therefore, the steps below do not need to be followed for every type of data breach. The situations in which the risk is high can be found at [Kluwereasyweg.be](https://www.kluwereasyweg.be).



1. If a breach comes to light, the **tool supplier (the data processor) must inform** the school (the controller) without unreasonable delay, providing as much information as possible. If there is a suspicion that personal data has been leaked and the breach therefore involves an increased risk, the school must be informed immediately.



2. Following the impact assessment, **the school (the controller) must assess** the data breach in terms of the rights and freedom of the students (the people concerned).



3. **Both parties** shall take the necessary measures to limit privacy violations wherever possible, and to avoid similar breaches in the future.

Among the measures that a school (the controller) must take, if the data leak is risky, are:

- Reporting the data leak to the DPA by submitting [a form](#) (© Data Protection Authority 2023, undated). Failure to report a data leak may result in a penalty. More information about the situations and how to report them can be found on [Kluwereasyweg.be](https://www.kluwereasyweg.be).
- Informing the students, parents, employees and other stakeholders.
- Updating the internal privacy policy to prevent similar data leaks in the future, even if the risk is low.
- Meticulously documenting every measure mentioned above, even if the risk is low.

Among the measures that a supplier (the processor) must take are:

- Supporting the controller as best as possible and providing assistance with their tasks. This can be done, for example, by providing access to the data or by sharing expertise.
- Updating the internal privacy policy to prevent similar data leaks in the future.
- Meticulously documenting each measure mentioned above.

This model processor agreement ensures uniformity and conclusive clarity for both the processor and the controller. **We therefore advise tool providers to build on this model every time a new contract is concluded with a controller school.**

2.5 BEST PRACTICE 5: IMPLEMENT A DATA POLICY

In our interactions with other EdTech tools, we noticed that the level of knowledge and the degree of implementation of privacy regulations is increasing. Many tools invest, among other things, in employees who develop and implement a privacy policy. On platforms, privacy statements are also given a prominent place more often. Furthermore, tools can increasingly count on the support of their own data protection officer (DPO), who is an expert in privacy legislation and GDPR.

However, there are also EdTech tools around whose data policies are not yet up to scratch. **If, as a tool provider, you have not done enough work to develop a sophisticated strategy, or none at all, the fifth best practice guideline is to do this work as soon as possible.** For every employee who comes into contact with data, it can be useful to be able to call on an IT coordinator or a DPO, or simply refer to a data policy to clarify any doubts they may have about an issue. Having such an expert can create a lot of clarity throughout the organization regarding the complicated tangle of privacy legislation.



HOW DOES IT WORK IN I-LEARN?

For its data policy, i-Learn called on the expertise of imec's Privacy Office, carried out a data protection impact assessment (DIPA) with an agency that advises on data policy (see appendix) and formally requested – and then applied – the advice of the Flemish Supervisory Committee. Specifically for the scientific research within i-Learn, the data policy was evaluated by the ethics committee of KU Leuven on the basis of a privacy dossier.

2.6 BEST PRACTICE 6: PERFORM A DPIA

Every new data processing task is unique and complex, and sometimes, as a tool provider, you have to move off the beaten track when it comes to data processing. Checking the data processing against your data policy does not always cover all the concerns that may exist about privacy risks. In such cases, it is recommended that you conduct a **data protection impact assessment (DPIA)**, which is the ideal check-up for your data processing.

Performing a DPIA is a way to uncover the possible risks associated with your data processing. A DPIA is not a fixed recipe that you can just follow. It is a well-documented process of thinking about the potential risks you run when processing data. The GDPR does provide a few guidelines that you should pay attention to (*Data Protection Impact Assessment*, 2021).

When exactly does a DPIA need to be done? This depends on the nature and scope of the processing and the possible impact on the rights of the data subjects. According to the GDPR, there is an increased privacy risk if (1) someone is systematically profiled on the basis of their personal data, (2) the data processing is particularly large-scale, or (3) the data is collected from camera surveillance in public spaces, for example. However, these are not the only situations in which a DPIA is needed. In order to keep an overview, the VTC has drawn up a list of all categories of processing for which a DPIA is mandatory (*De Vlaamse Toezichtcommissie*, 2022).

The responsibility for conducting a DPIA lies with the controller. It is up to them to ensure that a DPIA has effectively taken place and that the necessary measures have been taken to protect privacy. Consider, for example, an educational institution that uses a tool to process data on behalf of a school for a specific educational purpose. In the first instance, the school (controller) bears the responsibility and should not expect the tool (processor) to do this assessment.

However, it is not always necessary for the controller to carry out the DPIA itself. It can also choose to outsource the task to a third party outside the organization. In this latter case, it is important for the controller to keep a close eye on the process, however, and involve their own DPO closely in conducting it if possible.

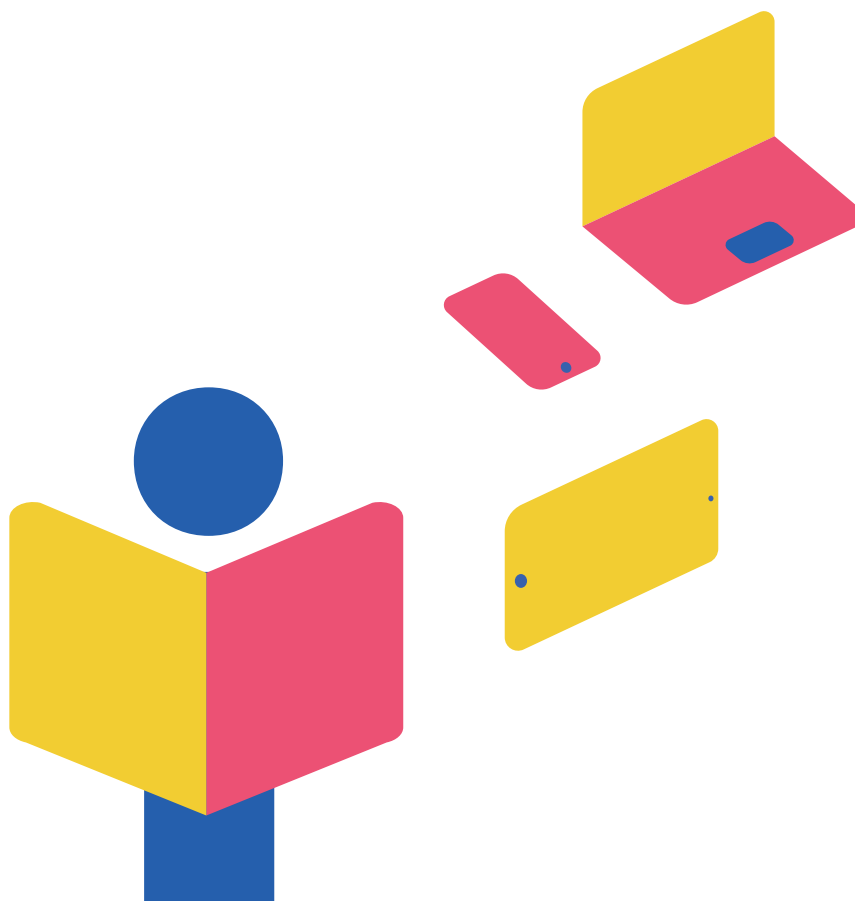
Even if you, as a tool provider, are not a controller, and it is not mandatory to have a DPIA conducted, it is very wise to do so in some cases. This is because it helps you to handle data carefully and to consolidate public trust. There is no requirement to publicize the fact that a DPIA has been carried out, but it can be good for the tool's reputation.

HOW DOES IT WORK IN I-LEARN?

The i-Learn project processes a lot of personal data belonging to students and teachers to enable personalized learning. It is crucial that this personal data is handled responsibly, given the sensitivity of the target group and the increased responsibility that the project has as a public contract. In order to guarantee optimal protection, i-Learn had a DPIA carried out on its own initiative. In this way, the privacy risks of the processing of personal data were properly mapped out and measures could be taken proactively to mitigate these risks.

i-Learn is a processor, and the processing responsibility (i.e. control) of the data itself lies strictly with the schools. As mentioned before, the implementation of a DPIA is the responsibility of the controller. Nevertheless, we decided to take the first step, and tried to help schools by carrying out an initial DPIA of our own processing practices. Schools that use i-Learn are welcome to use our DPIA to get a better idea of all the concrete privacy risks linked to the context of their own school.

Are you curious about the scope of our DPIA and what concrete findings have emerged from it? Please do not hesitate to read the appended report.



2.7 BEST PRACTICE 7: STAY INFORMED

A final golden tip and best practice guideline is continue thinking constantly about privacy and data protection. Every so often, in the wake of new technological developments, updated guidelines are drawn up and laws are altered. To keep up with this, you need to constantly stay informed.

To help you get started, we refer you to interesting documents and websites for tool providers, administrations, teachers and educational institutions with additional information about privacy rights, obligations and procedures.

Interesting documents and websites for tool providers (processor side):

- The declaration of intent *Privacy in Digitale Onderwijsmiddelen* and the accompanying model processor agreement: <https://www.privacyinonderwijs.be/>

Interesting documents and websites for teachers, school leaders and educational institutions (controller side):

- Het privacy-abc van Mediawijs, Vlaams Kenniscentrum Digitale en Mediawijsheid (Heyman et al., 2019): https://assets.mediawijs.be/2021-10/mediawegwijzer_privacy_herdruck19_def_lr.pdf
- Manual for reporting data leaks to the Data Protection Authority (DPA): <https://www.datenbeschermingsautoriteit.be/publications/handleiding-over-het-gebruik-van-invulformulieren.pdf>
- Step-by-step plan to successfully implement the GDPR in the policy of an educational institution: https://onderwijs.vlaanderen.be/sites/default/files/2021-07/In-7-stappen-naar-datenbescherming-in-het-onderwijs_Privacycommissie.pdf
- Guide to the GDPR for IT coordinators and school leaders: https://assets.vlaanderen.be/image/upload/v1664979613/wegwijzer_-_GDPR-AVG_q1qyel.pdf

3.

Conclusion

Let's return to the news article from the introduction. We asked ourselves whether the Flemish tool landscape was immune to data trading or data leaks. Through our contact with tool providers, educational institutions and data protection authorities, we can confirm that, generally speaking, a lot of effort is made to avoid abuses such as those that have come to light in the Netherlands. However, this does not mean that we can rest on our laurels and stop being constantly on our guard against irresponsible data processing.

We cannot ignore the fact that the use of data in education is showing an increasingly upward trend – an evolution that has been accelerated by the coronavirus pandemic. The amount of data we use to support our educational practice will not diminish in the future. So we still face many challenges in terms of data protection and ensuring privacy in education.

Below, we therefore focus one last time on the main challenge for education and offer some recommendations to policy makers, educational institutions and tool developers.

3.1 CHALLENGES AND RECOMMENDATIONS FOR EDUCATIONAL TOOLS

Some parties in the educational sector signed a privacy charter <https://www.privacyinonderwijs.be/overzichtslijst.html> back in 2018 and indicated to us that they use the associated processor agreement. However, the list of those parties is pretty limited and has not been updated since 2018, according to the [website](#). Since then, many new educational tools have appeared on the market.

Nowadays, a school must be able to handle a wide range of digital learning resources, without having to constantly ask itself whether the privacy of its students is being compromised. However, an up-to-date framework and privacy policy guidelines for these educational resources are lacking. These would not only reassure teachers but would also benefit the tool providers themselves.

In addition, it is a major challenge for providers of digital learning resources to keep up with the continually changing regulations around privacy. The constant changes in education, the digital world and the applicable regulations can be quite overwhelming. A charter may ensure that the GDPR and the privacy guidelines remain top of mind even so.

The question arises as to whether the standardization of a sectoral code of conduct or at least an exchange of information at different levels might offer a better solution. Based on our experiences in i-Learn and lessons learned from other collaborations, we would like to make a contribution and offer some recommendations aimed at suppliers and policy makers:

- **Recommendation 1:** The GDPR offers the possibility to draw up **sectoral codes of conduct** as a form of certification for a particular sector. This also applies to the providers of digital learning resources, who are then free to determine whether they want to comply with them. By drawing up such a code of conduct and having it validated by the Data Protection Authority, customers of digital learning resources can receive a certain level of guarantee with regard to privacy-related aspects.
- **Recommendation 2:** Another option is to **certify digital learning platforms through an independent organization** that establishes checks that the providers must undergo. If these checks are carried out transparently and regularly, schools can decide for themselves which digital learning resources they want to use. Transparent certification also increases transparency for parents and students because they can also view that information.
An example of transparent certification can be seen in the American use of ISO standards. It should be underlined that ISO standards are not a European concept.
However, European standards are being developed and are currently in the approval phase. These will also cover GDPR issues. Once the frameworks are available, it will be necessary to look at the possibilities for certification of EdTech companies in Belgium. Each country within Europe is expected to have its own certification procedures and standards, but ultimately those certifications must be EU approved.
- **Recommendation 3:** In addition, there should be **guidelines** for teachers so they can quickly evaluate whether it is safe to use digital learning resources such as free platforms and websites that are not subject to contracts. These guidelines can provide a limited overview of points of attention for teachers, such as the location of data processing and the use of cookies.
- **Recommendation 4:** Finally, it is important to give all school staff who come into contact with personal data access to **learning resources about its safe use in digital learning platforms**. If end users handle the data wisely, many privacy-related doubts can be automatically resolved, and risks can be avoided. For example, the learning resources may address limiting the data used and not always accepting all cookies.

Clearly standardization will never make the role of privacy experts in education superfluous, but it may help to focus their work on areas where it is really required. Regular validation and monitoring by data protection authorities will still be much needed, but the workload can then be shared between multiple parties.

3.2 RECOMMENDATIONS FOR TEACHERS AND SCHOOLS

If you are a teacher, it is important to remain vigilant about your students' data privacy when using a digital tool in the classroom. Admittedly, until a standardized framework is introduced, it will remain difficult to navigate the digital jungle successfully. Nevertheless, try to determine to the greatest possible extent what personal data is collected and how it is processed.



4.

Appendix 1: The DPIA for i-Learn

The i-Learn DPIA focuses specifically on the i-Learn MyWay portal, which processes data from both teachers and students. Since the project processes data from a sensitive target group and involves a large number of students under the age of 18, a robust data policy is essential. At i-Learn, we are also in favour of a *privacy by design* approach. This means that we have included the protection of personal data in the design of our platform and the development of our services from the outset.

To achieve this, i-Learn conducted an extensive DPIA to uncover and mitigate the potential privacy risks of the project. Based on the results of the DPIA, we were able to make a proposal for mitigation measures, which was then submitted to the Flemish Supervisory Committee. The committee's advice was embedded in i-Learn's data policy. In this appendix, we zoom in on the scope of this DPIA and discuss its results.

4.1 WHAT CAME WITHIN THE SCOPE OF I-LEARN'S DPIA?

Within the DPIA of i-Learn MyWay, we investigated the cloud architecture, the application, processes, approach, helpdesk, the optimization of the platform, maintenance, and the transfer of data from i-Learn MyWay. This appendix will discuss these topics further later on.

4.2 WHAT WAS BEYOND THE SCOPE OF I-LEARN'S DPIA?

The i-Learn project includes more than just the i-Learn MyWay portal. However, our DPIA only related to this portal. The following aspects were therefore beyond the scope of our DPIA:

- **The underlying (content) platforms** (Bookwidgets, Dodona, Smartschool, etc.)
- **The scientific research** (imec-itec-KUL)
- **The coaching platform** (i-Learn Academy)
- **The processing activities, risks and GDPR requirements** specific to the controller's role

Below, we briefly explain why these aspects were not included in our DPIA and, if relevant, what strategies we use to protect the privacy of our end users.

4.2.1 Underlying platforms

One of i-Learn's goals was to facilitate access to and use of educational content. i-Learn MyWay therefore provides schools with access to educational applications from a centralized platform. However, i-Learn does not host educational applications itself. MyWay's purpose is to ensure users find their way to external, third-party applications easily. This is why we did not perform a specific data protection impact assessment for all these external tools.

i-Learn nevertheless strives to increase awareness of and support for existing initiatives and to ensure that the data of its users remains secure and protected. For example, i-Learn provides a completed processor agreement or reference to the privacy policy for each application. For each individual tool that a school wants to use within i-Learn, the school administrator can view that processor agreement. The administrator can then very easily select the desired tools and include the agreements in the school regulations.

However, the way we provide the aforementioned support differs for each type of underlying platform or application that i-Learn works with. Thus we offer a brief discussion of the different approach to different tools, which we can classify into three categories: LTI-linked tools, complementary tools and class management systems.

- **LTI-linked tools**

LTI stands for Learning Tools Interoperability. When a tool is LTI-linked, it means that users can use the tool from i-Learn MyWay without having to log into it separately. These applications require the most personal data, because they create a personal account for each user and keep track of the user's progress, which allows monitoring by teachers and sometimes also by students themselves. For each tool in this category, i-Learn has concluded a processor agreement based on a model agreement, which is adapted to the specific requirements of the tool.

Some examples of LTI-linked tools available on i-Learn MyWay are:

1. **Bookwidgets:** As a teacher, you can use this tool to create various online exercises ('widgets'). It is an authoring tool that can be used for all subjects and ages.
2. **EduHint:** This tool offers digital maths practice materials for the first and second grades of secondary education.
3. **Karaton:** This is an educational adventure game, created to motivate children to practice reading and writing on a daily basis.

To access this category of tools, the school administrator must validate, sign and archive the processor agreements of the desired apps. i-Learn has also encouraged the third-party providers to sign the Declaration of Intent for Privacy in Digital Educational Resources. As a result, i-Learn has assessed these tools as having a high level of responsibility with regard to privacy.

FIGURE 3: To access i-Learn’s LTI-linked tools, the school administrator must validate, sign and archive the processor agreements of the desired tools.

Platforminstellingen

Gekozen platform
i-Learn

Verwerkingsovereenkomsten
i-Learn adviseert enkel akkoord te gaan met het gebruik van een tool als je de verwerkingsovereenkomst van deze partij accepteert. Door het bijhorende vakje in de tabel met tools aan te vinken, geef je aan akkoord te zijn met de verwerkingsovereenkomst. De verwerkingsvoorwaarden blijven steeds op i-Learn MyWay beschikbaar. Je kan indien gewenst het document downloaden, ondertekenen en voor eigen archief bewaren.
Wil je de tools van een aanbieder niet langer gebruiken? Neem dan contact met ons op via de helpdesk.

<input checked="" type="checkbox"/>	Akkoord	Aanbieder	
<input checked="" type="checkbox"/>	Ik ga akkoord	Wezooz Academy	Open >
<input checked="" type="checkbox"/>	Ik ga akkoord	Schooltv	Open >
<input checked="" type="checkbox"/>	Ik ga akkoord	La Digitale	Open >
<input checked="" type="checkbox"/>	Ik ga akkoord	Crunchzilla	Open >
<input checked="" type="checkbox"/>	Ik ga akkoord	DigiTAAL werkboek	Open >
<input checked="" type="checkbox"/>	Ik ga akkoord	i-Learn	Open >

58 resultaten

Bewaren

- **Complementary tools**

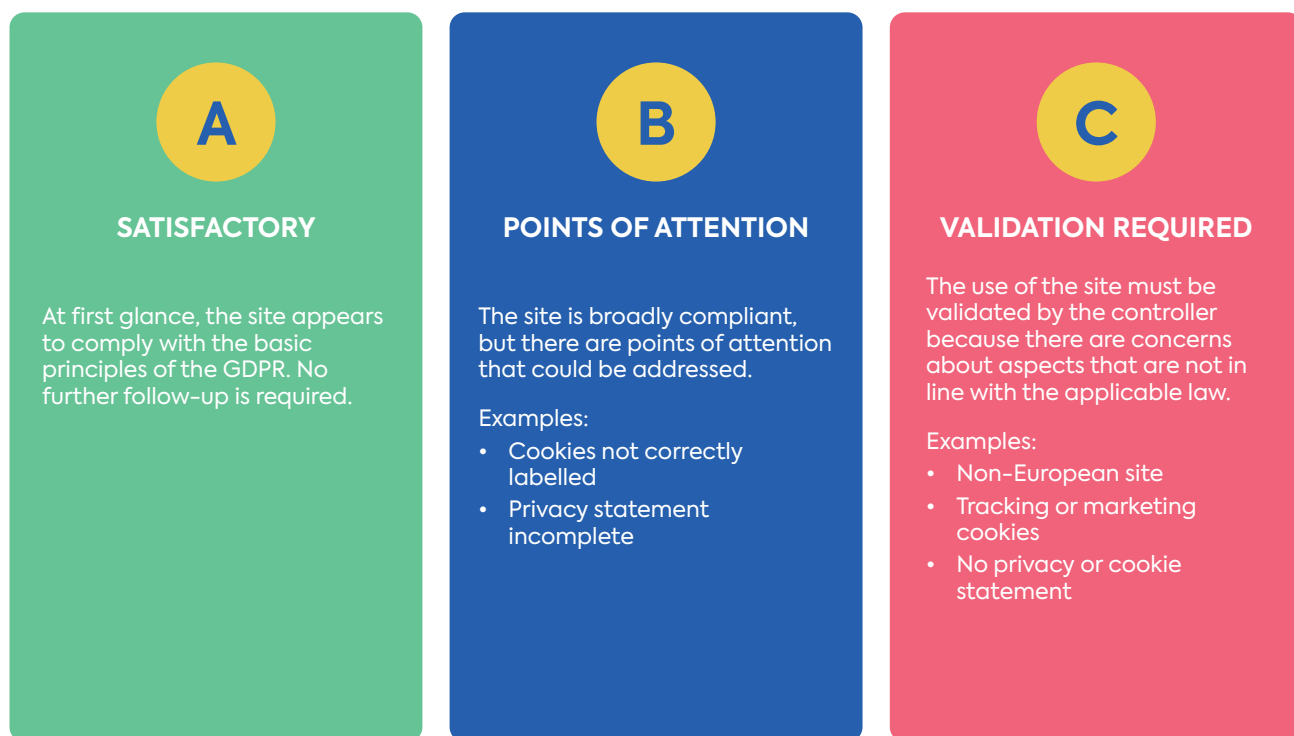
Complementary tools are freely accessible and do not require any personal data from students on the i-Learn platform. Although complementary tools are not directly integrated with i-Learn, they may still collect personal data in other ways through their own platform. For that reason, i-Learn also offers the privacy policy of these apps to school administrators. A school administrator must then validate that privacy policy before the tools are enabled. If an application is located outside the EEA and therefore follows privacy guidelines that differ from the GDPR, we will also inform the school administrator clearly of this.

In order to support schools in validating these tools, each complementary tool was also subjected to a privacy check by imec’s privacy office. This included checking the completeness of the privacy statement, checking the use of cookies and verifying whether data goes outside the EEA or not. If data goes outside the EEA, it means that it is subject to legislation other than the GDPR.

Based on our findings, we made decisions about any concerns or the need for further validation of the tool. The results of our privacy screening were then submitted to the tool’s designers so that they could make any changes required.

We can see an example of this process illustrated in our collaboration with the Universiteit van Vlaanderen (University of Flanders). The website initially received a negative assessment because the GDPR had not been applied correctly. The owners were contacted, and they made successful adjustments. The website is now fully compliant with European regulations. The tool has been part of the MyWay tool set ever since and is regularly consulted by our users.

FIGURE 4: The possible results of a tool review



- **Classroom management systems**

Teachers and students do not have to go to i-Learn every time to log in with a unique username and password. They can quickly access i-Learn through third-party identity providers such as Smartschool, Office 365, and Google. These class management systems ensure that the user (teacher or student) does not have to log in to i-Learn again, because they are already authenticated by logging into the system.

4.2.2 Research by itec

One of the pillars on which i-Learn is based is scientific research. The project was founded on existing scientific insights and aims to facilitate or generate new insights by using i-Learn as a testing ground for various issues. This research is carried out by the researchers of the imec research group, affiliated with KU Leuven (itec). Although data processing in such scientific studies is not included in the DPIA, strict measures are taken to ensure the privacy of the study participants.

Before scientific research can be carried out, the research must be evaluated **internally at KU Leuven** in terms of its ethical and privacy aspects. That is the task of the Social and Societal Ethics Committee ([SMEC](#)), which ensures that the research is in line with the GDPR (Research Coordination Office KU Leuven, 2023). Data processing may only commence once the research has been approved by the SMEC.

In scientific research using i-Learn, a second measure is also taken to protect the privacy of participants: personal data is pseudonymized so that the information collected is difficult to trace back to an individual. If a link has to be made between the information and the individual, explicit consent will be requested from the individual themselves or from their parent or guardian if the individual is a minor.

4.2.3 Coaching platform

A successful adoption of new tools is unthinkable without the necessary support for the users. In i-Learn, this is offered to teachers through the i-Learn Academy. Here, teachers can find online documentation and e-learning, as well as training and options for requesting on-site coaching and guidance. Since the processing of personal data on this platform is minimal and only adults (teachers) have access to this part of i-Learn, the Academy is not included in the DPIA. For example, only the surname, first name and email address are automatically stored in the Academy. If personal data is nevertheless requested, it is never mandatory to provide it, and explicit permission is asked. Teachers must also accept the terms of use and privacy policy once, before they can log in to the Academy.

4.2.4 Specific processing activities of the school

The school that uses i-Learn MyWay is always ultimately responsible for the processing of data. The processing activities of the school itself are of course specific to the school and can therefore not be included in the DPIA that the i-Learn project carries out. Each school must assess whether to have their processing activities inspected.

4.3 THE PHASES OF I-LEARN'S DPIA

In this section, you can read how the i-Learn team tackled the DPIA process for the MyWay portal, working with a specialist consultancy firm and imec's DPO. The process consisted of the following five phases:

4.3.1 Phase 1: Workshops

In the first phase, the consultancy firm spoke with various members of the i-Learn team, including the product owner, technical lead and programme manager, to get a clear picture of the portal and the data flow. Each workshop covered one specific topic that was explored in depth, such as the architecture, roles, legal grounds, transparency, and retention period of personal data in our portal. The results of all the workshops were bundled in a final document, the main conclusions of which are discussed further below.

4.3.2 Phase 2: Discussions

After mapping out the design of the i-Learn MyWay portal, along with the privacy risks associated with it and our strategies to mitigate those risks, we entered into discussions with various parties to present our plan. Based on the feedback we gathered during those conversations, we developed the first version of our DPIA.

We spoke to several schools and highlighted their potential role as data controllers for i-Learn MyWay. In addition, we researched tool providers to see if they could mitigate similar privacy risks in a better way. We also contacted the Information Security Working Group of the Flemish Department of Education and Training to present our findings and mitigation strategies, and we consulted this department's DPO.

4.3.3 PHASE 3: CONSULTATION WITH THE FLEMISH SUPERVISORY COMMITTEE

In a third phase, we asked for advice from the VTC. We presented our first version of the DPIA and in particular some privacy risks and strategies related to our cloud architecture. A highly developed cloud architecture, in which data is stored, processed and shared securely, is essential to guarantee the accessibility of digital resources in the classroom. For example, a powerful cloud ensures that i-Learn MyWay can deal efficiently and effectively with peak use during class hours and low use outside of school hours.

FINDING A CLOUD ARCHITECTURE: A QUESTION OF BALANCING FUNCTIONALITY AND PRIVACY

The advice of the Flemish Supervisory Committee (VTC) played a crucial role in finding a suitable cloud architecture for i-Learn. The VTC had rigorously scrutinized the use of American cloud services, such as AWS (Amazon), Azure (Microsoft) and Google Cloud, making it very critical of privacy (Van der Stadt, 2023).

The motivation of the VTC to take a hard line stemmed from various considerations. First, US companies have to comply with the Cloud Act and the Foreign Intelligence Surveillance Act (FISA), which essentially state that security agencies have the right to request data from any US company, regardless of the location of the server, in the event of a criminal investigation. In addition, schools process sensitive information, especially children's data. This further increases the importance of privacy and data protection.

i-Learn itself is not directly subject to monitoring by the VTC. Imec, the organization behind i-Learn, does not come under the VTC's jurisdiction. Nevertheless, we decided that it was wise to seek advice about our approach and cloud strategy from the VTC proactively. i-Learn currently uses Azure, an American cloud service.

As expected, the VTC advised us to avoid US clouds and to take appropriate measures. Although we recognized the value of US clouds for security and technical services that are not as well developed elsewhere, we also wanted to take heed of the VTC's advice. To minimize risks, we now store direct identifiers in a European cloud, while encrypted log and generated information is stored in the US cloud. Where possible, we aim to transition to European alternatives, such as the LeerID initiative. Through these measures, we reduce the risk for data subjects, while still using the functionalities of US cloud providers.

Because European cloud providers are less developed, we carefully weighed the pros and cons to make an informed decision that ensures data protection and privacy without sacrificing on functionality and technical advantages. Through our consultation with the VTC, we were ultimately able to find an appropriate balance between functionality and privacy in our search for a cloud architecture.

4.3.4 Phase 4: Last check by KU Leuven's DPO

After our consultation with the VTC, we finalized the document with our conclusions from the DPIA. That final version was validated by imec's DPO and aligned one last time with KU Leuven's DPO and the Flemish Department of Education and Training's DPO, after which we no longer required their services.

4.3.5 Phase 5: Permanent follow-up

Importantly, the completion of our DPIA was not an end point, but rather a starting point for ongoing privacy monitoring. Schools can use it to map out their own risks and better understand their responsibility as a controller. The i-Learn team will also regularly review the latest DPIA and update it as necessary, for example when new functionalities are added to the platform.

4.4 RESULTS OF THE DPIA

What have we learned from our DPIA? Based on the DPIA, we were able to divide the data that MyWay processes into three categories:

- **Operating data (category 1):** This is the absolute basic data that MyWay processes in order to be able to offer the portal to teachers and students. The category includes identification data and learning outcomes.
- **Optimization data (category 2):** This data is used to improve and optimize the MyWay portal. It includes feedback and user statistics.
- **Research data (category 3):** This data is collected for the purpose of scientific research into, for example, digital personalized learning. As indicated earlier, this was not within the scope of our DPIA.

For each category, we have made a brief analysis of the data processing, including its legal grounds and limitation of purpose.

Category 1: Operating data

For this category, the school is the controller and i-Learn MyWay the processor. Therefore, the legal grounds for processing operating data is usually determined by the school. Depending on the type of school, we recommend starting from the legal grounds of 'legitimate interest' or 'public interest'.

After determining the legal grounds, the school concludes a processor agreement with i-Learn MyWay, in which the obligations of i-Learn are also set down. i-Learn promises to limit the processing of personal data to what is strictly necessary and to limit access to it to those persons who need the personal data to keep the operation of i-Learn optimal. In that processor agreement, i-Learn must also be transparent about the tools it allows the schools to use. This means that the controller must accept a privacy statement for each linked tool.

Category 2: Optimization data

For this category, i-Learn MyWay is the controller. The legal grounds for the processing of this data is the legitimate interest of i-Learn MyWay to optimize the portal and add innovations to it. i-Learn always undertakes to carefully weigh up the importance of data processing in this second category against the potential impact on its users.

Category 3: Research data

Likewise for this category of data, the ball is in i-Learn's court. Depending on the type of investigation to be conducted, i-Learn invokes the legal grounds of consent and/or public interest. The study is always evaluated in advance by the Social and Societal Ethics Committee (SMEC) of KU Leuven and the privacy offices involved, and can only be started once all the necessary consents have been obtained.

Whatever type of data is involved, and whoever the processor is, we resolutely choose the most privacy-friendly approach for the processing of personal data in all these categories. Only those who really need the data for a clear purpose have access to it.












4.5 CONCLUSION AFTER THE DPIA














The DPIA process enabled us to map out the privacy risks of i-Learn. We considered mitigation strategies and implemented them as far as possible. We have also taken steps to raise awareness of privacy in education among i-Learn stakeholders.

The main findings of the DPIA process are that:

- Awareness of privacy issues has been increased among all parties involved. We notice that it has become a more prominent concern for all stakeholders, i.e. i-Learn project employees, stakeholders of the educational institutions, and the suppliers of the digital learning resources.
- Often, a failure to comply with the GDPR is not due to a lack of good intentions. It is rather the result of ignorance, time pressure or a scarcity of resources. Providing guidance and advice was usually sufficient to bring data processing in line with the GDPR, without the need for drastic changes.
- Deploying cloud infrastructure is an indispensable aspect of providing digital learning resources. However, this also entails a significant increase in complexity as a result of the complicated regulations that are associated with it.
- In the long term, providing personalized education will remain a challenging task in terms of data protection. This is because the demand for personalization will only increase, which will also increase the potential privacy risks. Addressing this issue and keeping all parties involved on the right track requires ongoing attention, time and resources.

Sources

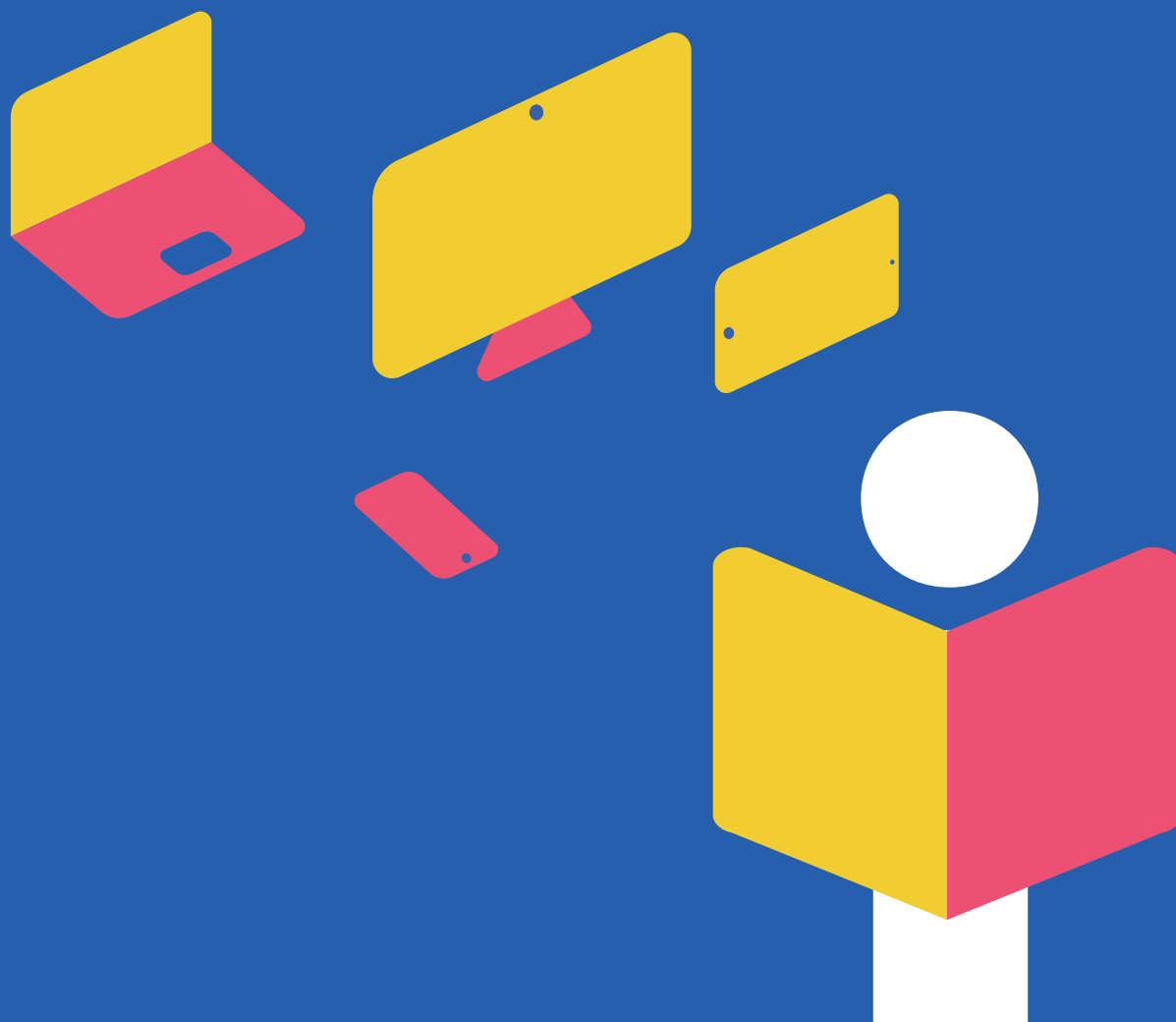
-  Berghmans, M., Decuyper, M., & van de Oudeweetering, K. (2020, 17 april). *Wat is goed digitaal onderwijs?* Platform L. Geraadpleegd op 17 mei 2023, van <https://ppw.kuleuven.be/platforml/blogs/2020/wat-is-goed-digitaal-onderwijs>
-  Burgess, M. (2020, 24 maart). What is GDPR?: The summary guide to GDPR compliance in the UK. *Wired UK*. Geraadpleegd op 23 mei 2023, van <https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018>
-  Commissie voor de bescherming van de persoonlijke levenssfeer & Vlaamse Toezichtscommissie (Reds.). (2018). In 7 stappen naar gegevensbescherming in het onderwijs: Volgens de Algemene Verordening Gegevensbescherming (AVG) van de EU. In *onderwijs.vlaanderen.be*. Geraadpleegd op 12 april 2023, van https://onderwijs.vlaanderen.be/sites/default/files/2021-07/In-7-stappen-naar-gegevensbescherming-in-het-onderwijs_Privacycommissie.pdf
-  *Data Protection Impact Assessment*. (2021). *privacycompany.eu*. Geraadpleegd op 19 april 2023, van <https://www.privacycompany.eu/knowledge-base-nl/data-protection-impact-assessment>
-  De ArgumentenFabriek (Red.). (2016). Omgaan met data in het onderwijs: Van en voor bestuurders in po, vo en mbo. In *kennisnet.nl*. Geraadpleegd op 23 mei 2023, van https://www.kennisnet.nl/app/uploads/kennisnet/publicatie/Omgaan_met_data_in_het_onderwijs.pdf
-  De AVG in het onderwijs: dit moet je weten: Veelgestelde vragen uit het primair en voortgezet onderwijs. (2019). In *yoursafetynet.com*. Media Security Networks BV h/o YourSafetynet. Geraadpleegd op 24 mei 2023, van <https://www.yoursafetynet.com/wp-content/uploads/2021/03/190523-YourSafetynet-AVG-vragenboekje-v5-Web.pdf>
-  De Vlaamse Minister van Onderwijs, Sport, Dierenwelzijn en Vlaamse Rand. (2020). Visienota "Digisprong": Van Achterstand naar Voorsprong: ICT-plan voor een kwalitatief digitaal onderwijs in uitvoering van het relanceplan "Vlaamse veerkracht". In *publicaties.vlaanderen.be* (VR 2020 1112 DOC.1425/1QUATER). Geraadpleegd op 23 mei 2023, van <https://publicaties.vlaanderen.be/view-file/40711>
-  De Vlaamse Toezichtscommissie (Red.). (2022). Beslissing VTC nr. O/2020/01 van 14 januari 2020: betreffende aanneming van de lijst met verwerkingen waarvoor een Gegevensbeschermingseffectbeoordeling dient te worden uitgevoerd conform artikel 35.4 van de Algemene Verordening Gegevensbescherming door Vlaamse bestuursinstanties. In *overheid.vlaanderen.be*. Geraadpleegd op 10 mei 2023, van https://overheid.vlaanderen.be/vtc_dpia_lijst
-  Digitaal Vlaanderen (Red.). (z.d.). *Digitale overheid: Digisprong in het onderwijs: Aanbeveling VTC bij de Digisprong in het onderwijs*. *overheid.vlaanderen.be*. Geraadpleegd op 23 mei 2023, van <https://overheid.vlaanderen.be/digitale-overheid/digisprong-in-het-onderwijs>
-  Gegevensbeschermingsautoriteit (Red.). (2023). *Melding van gegevenslekken: Een lek van persoonsgegevens melden*. *gegevensbeschermingsautoriteit.be*. Geraadpleegd op 27 april 2023, van <https://www.gegevensbeschermingsautoriteit.be/professioneel/acties/datalek-van-persoonsgegevens>
-  Han, H. J. (2023). "How Dare They Peep into My Private Life?": Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic. In *Human Rights Watch*. Geraadpleegd op 23 mei 2023, van <https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments>

-  Heyman, R., De Wolf, R., & De Geest, C. (2019). Het privacy-abc. In S. Hermans, E. Boudry, K. Linten, & H. Vanwynsberghe (Reds.), *assets.mediawijs.be* (D/2019/13.815/7). v.u. imec vzw. Geraadpleegd op 23 mei 2023, van https://assets.mediawijs.be/2021-10/mediawegwijzer_privacy_herdruk19_def_lr.pdf
-  Human Rights Watch (Red.). (2022, 25 mei). Governments Harm Children's Rights in Online Learning: 146 Authorized Products May Have Surveilled Children and Harvested Personal Data. *Human Rights Watch*. Geraadpleegd op 5 april 2023, van <https://www.hrw.org/news/2022/05/25/governments-harm-childrens-rights-online-learning>
-  Imec (Red.). (2022, 19 januari). Vlaamse EdTech-start-ups moeten – letterlijk én figuurlijk – over de grenzen heen durven te kijken: Imec-experten belichten de groeikansen voor (jonge) Vlaamse EdTech-bedrijven. *imec.be*. Geraadpleegd op 23 mei 2023, van <https://www.imec.be/nl/articles/vlaamse-edtech-start-ups-moeten-letterlijk-en-figuurlijk-over-de-grenzen-heen-durven-te>
-  Intentieverklaring Privacy in Digitale Onderwijsmiddelen. (2018). In *privacyinonderwijs.be*. Geraadpleegd op 23 mei 2023, van <https://www.privacyinonderwijs.be/Intentieverklaring.pdf>
-  Jvh & Blg. (2022, 23 december). Facebook schikt schandaal rond Cambridge Analytica voor 725 miljoen dollar. *De Standaard*. Geraadpleegd op 10 januari 2023, van https://www.standaard.be/cnt/DMF20221223_96167690
-  Model Verwerkersovereenkomst. (2018). In *privacyinonderwijs.be*. Geraadpleegd op 23 mei 2023, van <https://www.privacyinonderwijs.be/Modelovereenkomst.pdf>
-  Persbericht 'Modelovereenkomst beschermt persoonsgegevens in onderwijs' (Door A. Berckmoes, A. De Graeve, N. Jennes, K. Thijssens, M. Van Bogaert, & L. Van der Stockt). (2018, 22 mei). [Persbericht]. https://www.mijnclb.be/informatieveiligheid/downloads/2018_05_22_persbericht_gdpr_def.pdf
-  Prinsloo, P. (2020). Big data in education. The digital future of learning, policy and practice. *International Studies in Sociology of Education*, 29(1–2), 183–186. <https://doi.org/10.1080/09620214.2019.1690546>
-  Research Coordination Office KU Leuven. (2023, 2 februari). *Sociaal-Maatschappelijke Ethische Commissie (SMEC) - Social and Societal Ethics Committee*. *research.kuleuven.be*. Geraadpleegd op 30 mei 2023, van <https://research.kuleuven.be/en/integrity-ethics/ethics/committees/smec/documenten/index2>
-  Security.NL (Red.). (2022, 31 mei). “Meeste online onderwijsplatforms delen kinderdata met advertentiebedrijven”. Security.NL. Geraadpleegd op 5 april 2023, van <https://www.security.nl/posting/755384/%22Meeste+online+onderwijsplatforms+delen+kinderdata+met+advertentiebedrijven#:~:text=De%20meeste%20online%20onderwijsplatforms%20waar,onderwijsplatforms%20die%20door%2049%20verschillende>
-  Selwyn, N. (2015). Data entry: towards the critical study of digital data and education. *Learning, Media and Technology*, 40(1), 64–82. <https://doi.org/10.1080/17439884.2014.921628>
-  Van der Stadt, K. (Red.). (2023, 9 maart). Vlaamse Toezichtcommissie geeft vernietigend advies over AWS (update 13/10). *datanews.knack.be*. Geraadpleegd op 5 juni 2023, van <https://datanews.knack.be/nieuws/vlaamse-toezichtcommissie-geeft-vernietigend-advies-over-aws-update-13-10/>
-  van Trigt, M. (2019). Hoe data de kwaliteit van het onderwijs kunnen verbeteren. In *surf.nl*. Geraadpleegd op 23 mei 2023, van <https://www.surf.nl/files/2019-05/Whitepaper-Hoe-data-de-kwaliteit-van-het-onderwijs-kunnen-verbeteren-2019.pdf>

-  Verordeningen: Verordening (EU) 2016/679 van het Europese Parlement en de Raad: betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming). (2016, 27 april). Geraadpleegd op 9 januari 2023, van <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
-  Visienota "Digisprong": Van Achterstand naar Voorsprong: ICT-plan voor een kwalitatief digitaal onderwijs in uitvoering van het relanceplan "Vlaamse veerkracht". (2020). In *publicaties.vlaanderen.be* (VR 2020 1112 DOC.1425/1QUATER). De Vlaamse Regering - De Vlaamse Minister van Onderwijs, Sport, Dierenwelzijn en Vlaamse Rand. Geraadpleegd op 23 mei 2023, van <https://publicaties.vlaanderen.be/view-file/40711>
-  Vlaams ministerie van onderwijs en vorming (Red.). (2003). Bewaartermijn van leerlinggebonden documenten: SO/2003/02. In *data-onderwijs.vlaanderen.be*. Geraadpleegd op 23 mei 2023, van <https://data-onderwijs.vlaanderen.be/edulex/document.aspx?docid=13366>
-  Wegwijs in de AVG voor Onderwijsinstellingen: Uitgebreide technische brochure. (2018). In *privacyinonderwijs.be*. Geraadpleegd op 17 april 2023, van <https://www.privacyinonderwijs.be/TechnischeBrochure.pdf>
-  Wegwijzer GDPR/AVG. (2022). In *assets.vlaanderen.be*. Geraadpleegd op 25 mei 2023, van https://assets.vlaanderen.be/image/upload/v1664979613/wegwijzer_-_GDPR-AVG_q1qyel.pdf

iLearn

DIGITAAL LEREN
OP MAAT



INFO@I-LEARN.VLAANDEREN | WWW.I-LEARN.VLAANDEREN | WWW.I-LEARN.BE

on behalf of

umec

KU LEUVEN

itec

brightlab
shaping future innovators

IDLab
INTERNET & DATA LAB

 Vlaanderen
verbeelding werkt