European Education Area Strategic Framework

Working Group on Digital Education: Learning, Teaching and Assessment: 4th Peer Learning Activity (PLA), 19-21 March 2024, The Hague, Netherlands

Input paper: Recent developments in data protection and safeguarding privacy in digital education

"Recent developments in data protection and safeguarding privacy in digital education"[1]

1. Introduction

As a result of digitalisation, the use of education software platforms by schools, and consequently minors, has increased significantly in recent years. Increasingly, more (personal) data are stored and exchanged on digital platforms. Individual schools are faced with the task to assess and possibly mitigate privacy risks associated with data processing by large international software vendors, in order to comply with the European data protection rules (GDPR)[2]. If not properly done, personal data could be collected in education institutions without schools or individuals knowing. Protecting personal data is of course especially crucial for minors in schools. An important duty in this context is to conduct **Data Protection Impact Assessments (DPIA hereafter**)[3] as required under the GDPR for activities which are likely to involve "a high risk" to other people's personal information.

In both Flanders and the Netherlands, the national data protection supervisory authorities have announced the possible necessity based on the GDPR, to intervene significantly in relation to the use of certain commercial digital tools and services specifically developed for schools. Apart from the privacy risks at stake in education institutions, with possible negative consequences for learners, this is also relevant for national education ministries given the potential disruptive impact on the national education process and budgets. While the GDPR implies cooperation between the national data protection supervisory authorities, national education ministries should also be aware of such developments and ideally share experiences and knowledge.

Against this background, the Flemish and Dutch education ministers addressed this issue in a letter to the European Commission, which was also highlighted as a point of information at the last EU's Council of Education ministers (EYCS) under the Spanish Presidency, 23 November 2023. The letter suggested **supporting enhanced collaboration at European level,** to avoid the need for each member state to devote a significant amount of time, expertise and resources for negotiations with Big Tech firms in particular, and also requested the inclusion of this topic in the agenda of the European Commission. Commissioner Jourová, EU Commissioner for Values and Transparency and responsible for EU privacy regulation, has answered last February the letter to both ministers.

As a first step to further the discussion on privacy, this theme will be addressed and further explored in this PLA. This will make countries **better aware** of recent

[1] This paper has initially been informed by the experiences of the Dutch ministry of Education, Culture and Science (OCW) in their ongoing interactions with especially Google regarding the use of their products Google Workspace for Education and Chromebooks – as will be further elaborated by experts in the PLA – complemented later by similar developments in Belgium/Flanders and 3 other countries, see also **Annex I.**

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

[3] Data Protection Impact Assessment (DPIA) - GDPR.eu

developments related to data protection in relation to digital education in some countries, provide a **space for other countries** and others to share their knowledge and experiences. In this way, all participants should be in a better position to judge the **possible relevance of this issue** for their own national education policy. Secondly, the question will be what need and added value the members of the WG Delta see for additional support at EU-level, given the fact that currently exchange of knowledge, experiences and best practices between Education Ministries is still in an early phase. Thirdly, the discussion will also give the opportunity to identify other recent developments with impact on privacy of learners.

2. Developments in a number of EU/EEA countries

National agreements with Big Tech firms do not automatically apply in other countries

The central takeaway from the Dutch and Flemish cases is that improved conditions for the protection of personal data as agreed with international software vendors are not automatically applicable to (other education institutions in) other Member States/EEA Countries, despite the uniform legislative framework (GDPR). Even if suppliers are willing to grant permission for information to be shared between countries, this permission implies dependence on the supplier. Therefore, in each Member State, a significant amount of time, expertise and resources would potentially be needed to organise and/or facilitate similar negotiations. On the other hand, the outcome of the interactions in the Netherlands seem to have a positive effect on the disposition of software companies towards compliance with data protection rules, either directly (the outcomes are automatically part of contracts in other countries) or indirectly by setting a precedent for the outcomes of the risks analysis in other countries[4]. This depends however very much on the supplier. The question is whether such effects could be strengthened by improved exchange of information and knowledge between national education ministries and/or supervisory authorities.

National differences in governance of GDPR compliance in education and support to schools

In the context of the negotiations with Google and the preparation of the letter to the Commission, the Netherlands and Flanders have approached, including via the WG DELTA, other countries to gather information about similar developments in other European countries which are working within the legal framework of the GDPR. On the basis of the exchange of information and experiences, the situation and current developments in the *Netherlands, Belgium/Flanders, Denmark, Finland and Norway* are described in Annex 1.

In those countries, the actors responsible for complying with EU privacy regulation in processing personal data, differs between boards of education institutions and local/regional governments. This concerns, however, mainly the primary and secondary education sectors, and the situation in the VET and higher education sectors may even be more diverse between countries.

[4] How the Netherlands Is Taming Big Tech - The New York Times (nytimes.com)

In the 5 countries currently studied, there are - relatively recent - initiatives that have been taken to assist local/regional governments and/or school boards in their difficult task of GDPR compliance, by setting up and offering new support services and cooperation to jointly organize GDPR-compliance.

In the Netherlands, the programme *Digitaal Veilig Onderwijs* offers schools in primary and secondary education advice and support on (centrally) conducted DPIAs on commonly used software. The Dutch VET Council has set up a programme to commission DPIAs for the entire VET sector. For the educational institutions this has the advantage that most of the hard work of DPIAs is already done in central DPIAs, so they only have to assess their own processes in a local DPIA. However, a central DPIA does not take away the responsibility or ability for a school to do a full DPIA. For software suppliers, sector-wide DPIAs also provide great efficiency and financial advantage**.** On behalf of educational and research institutions (higher education) privacy and security risk assessments are conducted by SURF on suppliers.

In Flanders, under the responsibility of the Privacy Officers, a permanent governance body will be created to implement privacy audits on education software and mitigate possible privacy risks. This data protection expert working group in education consists of representatives (mostly DPO's) from the various education providers and umbrella organizations. The government, with the Digital Security Office of Digital Flanders, supports them with expertise to implement DPIA's, and the Digisprong Knowledge Center monitors their operations[5]. The Flemish government will also fund the generic DPIAs, in order to support individual schools and to relieve them of the planning burden.

In Denmark, the **Danish** Data Protection Authority took very recently a decision in the Elsinore/Helsingør case. In this decision, collaboration on joint assessments like DPIA's is encouraged. **Norway** has thoroughly examined the Dutch experiences with DPIA's and the recent developments in Denmark, leading to the development of a national DPIA on Google's educational products. The project is aligned with national authorities' efforts to describe and establish a general service for supporting local authorities in their privacy considerations within the school sector. This spring **Finland** is also piloting whether they could create central DPIA templates for the most common digital solutions used in comprehensive education.

Here the **key question for discussion in our PLA is how the dialogue and coordination are structured in your country between the different actors involved and what support is given to education institutions to comply with the GDPR**. The national efforts discussed could serve also as inspiring examples of the possibilities to other countries for national use or possibly also for similar approaches to be scaled up at European level (see hereafter).

Recent verdicts of national data protection supervisory authorities and courts

In the 5 countries studied, the national data protection supervisory authorities played a significant role, with a (potentially) *large impact on the education process and autonomy of schools.* For example, a decision by a national data protection supervisory authority to discontinue a certain intensively used device in the following school/

[5] More information can be found on this website (in Dutch): https://privacyinonderwijs.be/

academic year might result in considerable disturbance of the education process. In order to allow for a migration or exit strategy substantial investments in alternatives might be required as well. A complication however may be that, in practice, no good or easy alternatives with the same functionalities are (yet) available.

Some legal proceedings as described in Annex 1 have a lengthy history, and are still on-going and/or referred to higher court levels. An important issue in several cases concerns the use by the supplier of so-called **metadata for its own purposes**, also referred to as **diagnostic data.** Although such data are pseudonymized, they are indirectly identifiable, and therefore to be considered as personal data. Apart from such decisions on the outcomes of DPIA's, national authorities can also give fines to education institutions for not conducting a DPIA (for example, see Swedish case)[6].

3. Related issues and new developments with impact on privacy

Public alternatives as alternatives for Big Tech digital platforms

The fact that in the Netherlands, equivalent alternatives for the intensively used Google's Workspace for Education do not exist in the market did not strengthen the negotiation position of the Dutch negotiators vis-à-vis Google. The Dutch parliament has in recent years requested the Dutch government to explore, also at European level, the possibility of public, open source alternatives in education for digital platforms provided by the big technological firms. A common European approach in this respect would be a step in the direction of digital sovereignty from Big Tech companies, or at least contribute to more efficiency and a more equal power balance in the negotiations with them. At the moment, a number of EU countries is exploring the feasibility of a new European Digital Infrastructure Consortium (EDIC) focusing on creating 'digital commons' (EDIC-DC). In this context the potential for the education sector could be explored[7].

Influence of new product and technological developments

New products and technological developments could also result in new challenges for the education sector. In the Dutch Google Workspace for Education DPIA case for example, during verification of documentation by Google new, but less serious risks were discovered, which were the consequence of the further development of the product. SURF, SIVON and Google agreed to organize a continuing process to guarantee continued compliance with the GDPR. But bigger challenges may result from new technological and market developments like the increased use of algorithms and artificial intelligence in learning analytics and adaptive learning tools, including the

[6] Sweden: IMY fines Board of Education of Östersund Municipality SEK 300,000 for failure to conduct impact assessment | News post | DataGuidance

[7] **France and The Netherlands** are co-chairs, the working group further consists of **Estonia, Slovenia**, **Germany,** Austria, Belgium, Czech Republic, Italy and Poland (5 core Group Members in bold, other countries are observers). See regarding digital commons in digital education also the reference in the Council Recommendation on key enabling factors for successful digital education (23.11.2023).

new European legislation in this area which relates also to the rules in the GDPR[8]. **Education institutions should adapt their internal policy and management processes accordingly, and also invest in the professionalization of their staff.** They must (learn to) act on the basis of the preconditions needed to make good use of ICT in education: vision, expertise, content and applications, and infrastructure must be in line with each other. When these building blocks are well aligned and balanced with each other, the desired returns in the field of ICT can be achieved. Information security and privacy are preconditions in the choice of software, and should not be negotiated in a subsequent process with the software supplier, but ideally in advance when choosing the software or supplier.

Privacy beyond GDPR-compliance

It is important that the discussion of privacy in digital education does not revolve entirely around technical and legal compliance issues in relation to the GDPR, but also considers what rights for children we want to protect, and how this may be infringed by ICT-tools being introduced into the classroom. The Flemish *Kenniscentrum Digisprong* has already published recommendations to schools about how to consider the use of monitoring software which has, of course, a big impact on the privacy of children[9]. The Dutch organisation *Kennisnet* has recently worked together with the Universiteit Leiden and UNICEF Netherlands to increase awareness about these issues and give guidance, advocating also for a '(data) free space in school'[10]. In the Netherlands *SIVON*, on behalf of primary and secondary education, has included a "Best Interest Assessment" in their DPIAs to assess the impact of the examined software on children's rights.

4. A common way forward?

The European legal framework and basis for consistent application and enforcement

Commissioner Jourová has emphasized in her recent answer to the Dutch and Flemish Education Ministers that the EU has a strong legal framework for the protection of personal data and privacy. In this context, the DPIAs provide a useful tool for data controllers to assess the necessity and proportionality of the envisaged processing, the possible risks related to this processing, as well as appropriate measures to address these risks. National data protection supervisory authorities have an important role to play in monitoring and enforcing the application of the GDPR in the Member States. They also have the task of promoting the awareness of controllers and processors of their data protection obligations and to advise, in accordance with national law, national authorities on measures relating to data protection. With a view to ensuring consistent application and enforcement of data protection rules, *national supervisory authorities shall cooperate with, including sharing information and providing mutual assistance to, supervisory authorities in other Member States*. At the

[8] E.g. (in Dutch): Sectorbeeld Onderwijs 2021-2023 | Autoriteit Persoonsgegevens

[9] https://www.vlaanderen.be/kenniscentrum-digisprong/themas/veiligheid-privacy-welbevinden/monitoring-van-digitale-toestellen

[10] Data-in-de-klas-Essay-3.pdf (unicef.nl)

Union level, the consistency of EU data protection framework is also ensured by the European Data Protection Board (EDPB)[11].

Aligning national actions under the Digital Education Plan?

As mentioned in the reply by Commissioner Jourová, an *exploratory discussion aligning national actions to protect and secure data privacy could be included in the reflections on the review of the Digital Education Action Plan*, which the Commission will launch early 2024. The EU could foster a collaborative and coherent approach to data protection and security in educational technology across Member States. This letter also suggests that our DELTA working group could also provide a forum for ongoing dialogue and for sharing experience and good practice, as we are initiating now in this PLA.

In parallel to the gathering of information by the Netherlands, the Finnish Education Ministry has sent several Member States a survey on this issue, in order to produce a summary of *legislation and guidelines* implemented by other EU Member States on this compliance with GDPR, and also to identify possible additional guidance methods in other countries. The analysis of this survey (currently answered by 7 MS) is still ongoing and should be finished by spring of 2024.

A next opportunity for Member States to discuss the topic of privacy in digital education after this PLA, and give guidance at a more strategic level, will be the *Digital Education Dialogue* organized by the Belgian Presidency with support of the European Commission (Gent, 28-29 May 2024).

Questions for debate in the Pear Learning Activity

National experiences

1. Has the issue of data privacy, in relation to teacher and student data being stored and reused on digital platforms and compliance with the GDPR, come up in your country as an issue and if so, how? How is the dialogue and coordination structured in your country between the different actors involved and what support is given or being considered for education institutions to comply with the GDPR? Have any initiatives been undertaken in your country to develop public alternatives for large commercial software vendors?

Aligning national actions, additional action at EU-level

[11] EDPB | European Data Protection Board (europa.eu)

2. What would be the need or added value (if any) for additional coordination and exchange of experiences, knowledge and tools in this area at European Union level? How could this be best organised in relation to the remaining period of the Action Plan Digital Education 2021-2027, the implementation of the recently adopted Council Recommendation(s), the (future) mandate of our DELTA working group and the role of national supervisory bodies and European privacy bodies as based on the GDPR?

Annex I: Examples in a number of EU/EEA countries

The Netherlands: Google Workspace for Education case

In the Netherlands, educational institutions have a high level of autonomy, including in regard to the procurement and use of digital education tools and platforms. These institutions operate under boards, which are responsible for the quality of education and all things related to that fall under their jurisdiction. In this governance context, Dutch educational boards are data processors in the sense of the DGPR and as such also carry a responsibility for the privacy of their pupils, students and employees, in relation to the European date protection rules (GDPR). This duty of care means that they should have control over students' personal data. However, for individual school boards in primary and secondary education it is - increasingly - complex to assess such risks adequately, especially when they are using products of big technology firms like Google and Microsoft. The publicly funded ICT-cooperative SIVON has been tasked under the programme Digitaal Veilig Onderwijs to act on behalf of school boards and support them in the difficult task to assess data protection risks. SIVON has published a fully aligned DPIA-process for schools[12] and software suppliers[13]. Furthermore, SIVON conducts checks on data processing agreements of commonly used systems in primary and secondary education[14].

In 2020, the Dutch Ministry of Justice, together with the University of Groningen, the University of Applied Science of Amsterdam, SURF and SIVON completed a DPIA on Google G Suite for Education (later renamed as Google Workspace for Education)[15]. This DPIA resulted in the conclusion that the use of Google Workspace for Education carries several privacy risks for the Dutch schools. **An important risk concerned the use of metadata.** Google had the point of view that it should itself be the only actor responsible for processing metadata, meaning that Google will determine itself for which purpose data are collected; how this will happen and will be able to change metadata without consulting users. This would mean that schools would have no grip on what would happen with the data collected while using the product. **Other risks** included the lack of legal grounds for data gathering, the risks related to data transport to countries outside of the EEA, and a general lack of transparency[16].

In July 2021, an agreement with Google was reached to mitigate all risks in the Netherlands no later than 31 December 2022. In December 2022, Google delivered their documentation. However, a verification report indicated that 6 out of 9 risks as found earlier in 2021 were not adequately resolved. As a result, SURF, SIVON and the Ministry of Justice proposed a new ultimatum or otherwise Google Workspace would be considered to be acting in conflict with the GDPR. Google agreed to this. In the summer of 2023, Google delivered documentation on their promise to mitigate the risks in the Netherlands. In the summer of 2023, a final agreement was reached with Google after verification that the most important risks as identified in 2021 (8 out of 9) had been adequately addressed, as confirmed by the Dutch national data protection supervisory Authority (AP). Beginning 2024 the last remaining high risk - the 9th - has been resolved after assessing the data transfers and finishing the data transfer impact assessment (DTIA). Also, five newfound risks were addressed and mitigated. SURF and SIVON have entered a new phase with Google with completion of the DPIA, DTIA and new findings, with new developments and legislation being discussed during a monthly meeting with Google's education team.

The Netherlands: privacy sector-analysis education sector

Apart from the specific Google-case, the Dutch data protection privacy authority (AP) plays an active role in following the developments in the Netherlands regarding data privacy in education. Following a round table with educational institutions, it presented at a recent National Privacy Conference[17] a "*Sector analysis of the education sector in the period 2021-2023"*.

In this analysis, challenges for education, including new developments like the increased use of algorithms and artificial intelligence in learning analytics and adaptive learning tools were presented[18]. Education institutions should according to the AP not wait for the implementation of the EU's AI Act, but already start preparing their internal policy and management processes. Also, the education sector should work toward enlarging AI knowledge among teachers as a guarantee for a responsible use of algorithms in education.

Belgium/Flanders

Also in Flanders, Belgium, school boards have a lot of autonomy in choosing platforms and systems. The data protection field is rather fragmented, with seven data privacy officers (DPO's) active in the country. The Flemish privacy authority (VTC) has been in extensive discussions with Google and was not convinced by Google's answers. Therefore, the VTC advised the discontinuation of use for schools who had implemented Google Workspace for Education services in all layers of the school. Questions remain around the strictness and monitoring of the discontinuation.

Following the VTC's recommendations, a proactive approach was adopted to ensure the privacy of Flemish educational data. A working group comprising the seven data privacy officers (DPOs) was established to facilitate a comprehensive dialogue between educational stakeholders, including Google. This initiative aimed to create **a permanent governance body** to implement privacy

[12] Data Protection Impact Assesment - SIVON

[13] https://sivon.nl/dpia-leveranciersinformatie/

[14] https://sivon.nl/toetsen-verwerkersovereenkomsten-2/

[15] As part of this exercise, Privacy Company had done technical and legal research into the data Google processes when Google Workspace is used on mobile phones with the iOS and Android operating systems, on a Chromebook running ChromeOS, on a Macbook and on laptops with Windows 10.

[16] Privacy assessment Google Workspace (G Suite) Enterprise : Dutch government consults Dutch Data Protection Authority on high privacy risks - Blogpost (privacycompany.eu)

[17] Nationale Privacy Conferentie 2024 - ECP | Platform voor de InformatieSamenleving.

[18] Sectorbeeld Onderwijs 2021-2023 | Autoriteit Persoonsgegevens

audits on education software and mitigate possible privacy risks. This new approach ensures a balanced approach to the adoption of digital educational tools that safeguards student and staff privacy. This data protection expert working group in education consists of representatives (mostly DPO's) from the various education providers and umbrella organizations. The government, with the *Digital Security Office* of Digital Flanders, supports them with expertise to implement DPIA's, and the *Digisprong Knowledge Center* monitors their operations[19].

Denmark

The Danish DPA imposed 14 July 2022 a ban on the use of Google Workspace in the Elsinore municipality. After two years, the Danish privacy authority has come recently (30 January 2024) to a decision in this Google Workspace for Education case, which started in the city of Elsinore/Helsingør. The case revolved around the question of whether Elsinore county (and 52 other counties) had a **lawful basis when they issued Chromebooks to pupils**. The use of Chromebooks by the counties entailed an array of agreements between the counties, the pupils (or rather their parents) and Google, some of which made Google the data controller for certain sets of data. This is mainly what was termed "Service data" – the lawful basis for using Google as a processor for customer data (i.e. documents, forms, etc.) was never in question.

The counties' main argument was that they had lawful basis for these additional uses because of their interest in the ongoing development and refinement of the teaching tools they used (i.e. GWSfE, Chrome EDU Upgrade, etc.) The verdict did not accept this argument with the decision hinging on the question of whether the processing was "necessary". The verdict suggests three different ways for the counties to proceed: 1) Google developing the technical means to cut themselves off from data, 2) amending agreements with Google, or 3) Danish parliament supplying the needed lawful basis. Each of the 53 counties named have until March 2024 to indicate to the Danish privacy authority how they intend to proceed and until August 2024 to comply.

Finland

The Finnish Ministry of Education is steering towards a comprehensive digitalization strategy in early childhood education and care (ECEC), pre-primary, primary and lower secondary education. This includes guidance related to both the use of digital devices and software in teaching and the increasingly widespread processing of personal data in digital learning environments. In December 2023, the document "*Target state of digitalisation in early childhood education and care, pre-primary, primary and lower secondary education*"[20][1] was published.

There is an ongoing court case on the use of Google Workspace for Education in comprehensive education. In 2021, the Finnish Data Protection Ombudsman issued a decision on a query from a private citizen from 2018 regarding the use of Google Workspace for Education in teaching and learning. The Ombudsman stated that the processing of personal data by one of the education providers using Google's learning environment had been contrary to the GDPR. In terms of the legal basis for processing personal data, Article 6(1) (c) of the GDPR (the controller's legal obligation) could not be used as the legal basis for *all* personal data processed in Google Workspace for Education.

After this, the case was appealed and moved to the Administrative Court. In June 2023, this Court issued a decision stating that the Article 6(1)(c) of ***the GDPR is not suitable as the basis for processing personal data to the extent proposed for Google Workspace for Education,*** and the processing of personal data by the controller has in this respect been contrary to the GDPR. The education provider appealed against the decision. The Supreme Administrative Court is expected to decide this spring 2024 whether it will take the matter up for consideration.

Norway

The Ministry of Education of Norway steers schools through the Education Act and the core curriculum. Municipalities (primary and secondary level) and county municipalities (upper secondary level) own the schools and decide what learning resources can be used.

After the pandemic, Google Workspace for Education has been used in more than 20% of public schools. The Norwegian Association of Local and Regional Authorities (KS) translated the Dutch DPIA as a backdrop to the ongoing work, and developments in Denmark/Helsingor (including a problem with YouTube) were also closely monitored. Now, KS and Bergen municipality have initiated a project to attempt to create a national DPIA of Google's products and services in schools, partly funded by national authorities. The plan is that the DPIA will be completed in an 80 per cent version. Approximately 20 percent of the work will remain to be completed by each municipalities using the assessed Google services. The municipalities are responsible for processing personal data according to data protection legislation, and hence it is the municipality that must take ownership of its DPIA. The overarching goal is good governance by municipalities (357 in 15 regions; the smallest have less than 1000 inhabitants). Further information can be found on the KS website.[21]

The project is aligned with national authorities' efforts to describe and establish a general service for ***supporting local authorities in their privacy considerations within the school sector.*** These national efforts are justified by the costly, duplicated and parallel work local authorities are doing in conducting privacy assessments of all digital services and solutions that are used in the school sector. The proposed support service is likely to include a range of privacy and GDPR-specific demands, such as drafting sectorial DPIAs and assisting in the process of mandatory risk-evaluations. Additional to the support service, a national service catalogue for digital learning materials will be established, where the product evaluations conducted by the privacy support service will be visible.

[19] More information can be found on this website (in Dutch): https://privacyinonderwijs.be/
[20] https://julkaisut.valtioneuvosto.fi/handle/10024/165321

[21] Receive weekly updates about our project of making a national DPIA for Google products used in school - KS