Report of the International Working Group on Digital Education – September 2017

39th International Conference of Data Protection and Privacy Commissioners in Hong Kong

Foreword:

As Group Moderator, I would like to extend my sincerest thanks to the New-Zealand Office of the Privacy Commissioner for the sterling work done by the ICDPPC Secretariat staff and enhanced support he brought to the visibility of our Digital Education Working Group, in particular:

-By dedicating **a specific space on the international conference website** to our activities and group reports, and indexing our key initiatives which allowed us to communicate within and outside our Data Protection Authorities community as well,

- By regularly publishing in the ICDPPC Newsletter states of progress of our working group's activities,

- And in terms of innovation, by launching the **First Global Privacy and Data Protection Awards in 2017**, which highlighted 46 creative initiatives from our authorities in the field of Privacy Education intended for public audiences, Youth and the educational community.

In 2017, the DEWG expanded to **54 DPAs members, representing 6 major zones of the world:**

- **Europe: 31**
- **Africa: 8**
- **Asia-Pacific: 6**
- **North America: 4**
- **Latin America: 4**
- **Near / Middle East: 1**

We would be pleased to welcome other authorities who would like to join our work.

This report seeks to take stock of the three main actions of the working group's **2016-2017 action plan program**, and put forward a new roadmap for the coming year to be agreed by our DPA colleagues [in pursuance of the objectives related to the Warsaw and Marrakech resolutions in Digital Education.

This year, the action plan program was based primarily on the implementation of *the Marrakech Resolution for the adoption of an international Competency Framework on Privacy Education* (October 2016). That is to say on two priorities focusing as a follow up of actions covered by digital education activities, including providing new resources to the Competency framework and a third focus suggested to deal with e-Learning platforms and educational online services.

1. **Implementation of the Competency framework on Privacy Education in study programs and curricula, including organising it through use of available teaching resources in accordance with age-groups concerned and proposing pathways for training educational staff;**

2. **Evolution of the services and content of the CIRCABC web platform with sharing digital education resources concerning protection of personal data and making the educational resources base available to the educational community;**

3. **The question of development, and widespread use on the part of the education community of eLearning platforms, online services and applications dedicated to the education community with regards to privacy issues.**

Action 1: Implementation of the Competency framework on Privacy Education in study programs and curricula, including enhancing it with teaching resources in accordance with age-groups concerned and proposing pathways for training educational staff (*See the PowerPoint presentation*)

Objective: To ensure proper coordination and report on states of progress related to the implementation of the framework at national / regional levels by DPAs

Feedback information related to this action shows a strong mobilization committed by a large number of authorities (27 DPAs) and in particular, exploring partnership opportunities with national educational actors to include the international competency framework with appropriate resources in school curricula and teacher training.

- Media coverage of the framework, dialogue with the relevant education authorities and integration into curricula

The competency framework has been largely promoted on the DPAs websites and social media also via special co-organized events in schools and during the Safer Internet Day (in February 2017). Many countries have contacted their relevant ministries (of Education, Innovation, Digital Strategy) [1] or even their national parliament[2] in order to fully prepare the integration of this framework into curricula.

In this purpose, it has been translated in six more languages, namely, Albanian, Catalan, Hungarian, Italian, Polish and Spanish (in addition to French and English).

The collaboration and partnerships with education authorities have been strengthened and resulted in reform projects that will encompass the topic of digital education, conducting an audit and listing all existing actions on data protection in classes and in curricula, creating working groups with the Ministry to develop the framework and supplement it with relevant resources and capacity (human and financial) tailor made to each academic cycle, or developing online tools to enable to navigate through the competences of the framework (see the PowerPoint presentation by CNIL).

- Feedback from school and other field partners, promotion of the use of the framework in lessons practices, adaptation of resources by competency and age groups

The feedback was particularly positive from schools on the use of the competency framework in the context of training workshops organized with students and their parents[3]. A review of teaching resources available in schools has been conducted in order to identify any remaining gaps between existing lesson plans and the framework, and develop appropriate training materials to address them[4].

- Development of initial and ongoing training for teachers / supervision

If the framework is considered as a useful basis to structure teachers' approaches, numerous countries are considering more developed programs to raise awareness amongst teachers school leaders and parents (e.g. *new videos on digital skills acquisition have been developed for a family training plan*[5]*)*. Training modules are conducted targeting teachers and school directors on the fundamental data protection principles aimed at national vocational education, other useful contacts are also made with University to develop training for teachers, and the National Education Training Institute[6]. Other online training programs are currently being prepared to be made available to teachers, supervisory staff and school leaders[7].

[1] ALB / CA / CAT/ CH/ CY/ CZ / EE/ FR/ GI/ HU/ IT/ LU/ MLD/ ML/ MU/ MX/ ONT/ PL/ SN/ SP

[2] MX/ SP

[3] ALB/ CAT/ CY/ FR/ GI/ GR/ HU/IR/ LU/ MD/ MX/ SN/ SP

[4] ALB/ CAT/ CY/ FR/ GI/ GR/ HU/IR/ LU/ MD/ MX/ SN/ SP

[5] CZ/ FR/ GI/ SP

[6] FR/ LU/ALB/ MX/ SN

[7] FR/ LU/ SN

- Postponed initiatives

Some other DPA offices informed us of having no plans at current stage with regards to this issue, but will consider the possibility of prioritizing it in the future while further developing their current yearly awareness program with school partners[8].

With regard to follow-up actions for 2017-2018, (as another major challenge related to this outcome), I suggest:
→ The DPAs continue the exchange of experiences to build on successful and replicable initiatives to integrate into school curricula the teaching of a culture of protection of privacy and personal data through the framework and other key inputs essential to dissemination of a digital citizenship culture
→ **Discussing** if it could be relevant to consider adopting an enhanced version of the framework, sequenced by age groups concerned, complemented with examples of adapted resources, where appropriate, and on condition that the advanced progress of the work allows it?
→ The DPAs provide teaching aids and classwork on the one hand, and training pathways in the field of digital education to the beneficiaries of teachers and educational staff on the other hand (*in the form of e-Learning or any other teaching method*).

Action 2: Providing the CIRCABC web platform with new services related to content sharing in digital privacy education and making the educational resources base available to the educational community

Objective 1: **Encourage sharing of resources between DPAs facilitated by the use of the CIRCABC platform**

34 registered users only with the status of contributor DPAs are registered on the CIRCABC platform (i.e. a total of 26 DPAs registered).

Updating the online library (main input):

- Provided some 50 additional resources uploaded in 2017 incorporating a brief summary of its content downloaded by CNIL [in French and English]
- Added a section dedicated to "Parents Guides"
- As a matter of fact, very few DPAs have uploaded new resources during the year and access registered to the website is also unstable (*some 400 logs - it can vary from 5 to 118*

[8] BE/ GR/ MK/ MO/ EE

views per month corresponding to the maximum of CNIL's activities of up loadings materials on the platform in July 2017)

- Online publishing of a detailed plan of the site (a mind map) aimed to facilitate easy navigation and classification in the current architecture of the platform
- Sending notification to the registered members on CIRCABC on new materials uploaded has already been tested. This would make members of the interest group more aware of new content on the platform and raise interest in the uploaded documents (*outstanding operational functioning offering the possibility to its members to accept or refuse any further notification*).

Main figures: **240 documents uploaded in various languages**, among which:

- Varied teaching and training quality resources providing *mixed ready-to use kits for teachers and students (with online training material, quizzes, articles, working documents, exercises, games, etc.), guides and ideas for practical cases for the classwork, videos, posters, comics, thematic factsheets, vademecum for students/ teachers; 2017 study report on key resources for DPAs, competency framework, parents' guides*.
- The potential for more than hundred quality resources identified for further uploading which might include educational thematic series sequenced by age groups concerned (sourcing from DPAs internet-based websites, ICDPPC listed inventory for the Awards, national and international institutional sites)
- But there has been very little input on the part of DPAs.

Objective 2: **Explore the opportunity and feasibility of making the CIRCABC educational resources base available to the educational community**

This initiative could concern all or part of the educational resource base to be downloaded from accessible public website to the educational community in Europe and beyond. This can include, for example, an international website specialized in data protection and/ or web portals already providing educational resources.

As first feedback information, the public portal "Open Education Europa" (OEE) www.openeducationeuropa.eu/ grants access to existing Open Education Repositories / (OER) free of copyright resources in Europe and beyond. The community includes some 20 000 professionals interested in e-Learning.
The CNIL has tested and uploaded the competency framework on OEE platform which is currently well placed on the homepage among downloads of recent news. It results that a specific section dedicated to data protection and privacy topics could be opened up in January 2018 by OEE platform's administrators if we plan to supply it with more contents.
This platform is open to all European and non-European countries in the world.

It will now be a question of discussing the value of available free of copyright resources and the attractiveness of this OEE platform for targeting teachers and reviewing the workload to achieve it.

With regard to follow-up actions for 2017-2018 in order to facilitate the sharing of resources to implement the competency framework, I suggest:

→The DPAs continue uploading pedagogical materials in the field of data protection on CIRCABC platform, i.e.
Complement CIRCABC with resources for teachers' lessons and more specific content to support teachers' vocational training paths for each area of knowledge and skills covered by the training competency framework

→ Create a small steering group to establish a call for expression aimed to conduct with CNIL and CNPD (Luxembourg Commission) a study extended to alternate educational portals.

Action 3: The question of development, and widespread use on the part of the education community of eLearning platforms, online services and applications dedicated to the education community with regards to privacy issues.

Many of e-Learning platforms and educational services facilitate collaborative learning and communication, but in doing so, also collect vast amounts of sensitive personal information about students, including behaviours, attitudes and students' personal data. But, are students' personal information appropriately protected?

A detailed questionnaire was circulated on 15 July 2017 to all accredited Authorities on behalf of the Canadian OPC acting as current lead in this action with CNIL's commitment.
The survey aimed to examine "the question of development, and widespread use on the part of educators and their students, of eLearning platforms and online services and applications dedicated to the education community, developed and made available online, usually free of charge, by private service-providers, and raising (as in another sectors) issues with regard to collection of students' personal data, from minors in particular."

Outcome: Refer to the annexed document which will be presenting full outcome of the survey and proposals of recommendations by OPC of Canada.

Follow-up of the 2016 action: Publication of a competition guide for Youth on data protection

The DEWG has just published **a methodological guide to organize youth competitions on data protection.**

About this guide

This guide is designed as a *checklist* that identifies essential points to keep in mind when launching and conducting a competition. It describes in detail the questions to ask oneself for each point of the competition, *such as budgetary or communication issues, seeking for media partners, assessment criteria of applications for the jury, Prize-giving ceremony, annual assessments of the competition as well as risks management strategies.* It then gives some practical advice in relation to all of these aspects.

The guide has been conducted by **the French CNIL and the Czech Office for Personal Data Protection** and with the valuable assistance of the data protection authorities which had already held national competitions designed for young people[9]. It will be posted by end of September 2017 on the website of the international conference on behalf of the DEWG and will be accessible as a free of copyright resource.

Who should use this Guide?

The guide aims to assist Data Protection Authorities wishing to undertake organisation of competitions intended to young people. It is a very nice challenge to promote within the framework of a competition, highly creative and innovative scenario developed by and intended for young people as peers, which aim to provide good practices to protect one's Privacy on the Internet. [For the last 3 years, the CNIL has been conducting in cooperation with the Digital Education Collective of actors the "Educnum Trophies" awarding and further accompanying young people aged between 18 and 25 in the development of innovative projects, embracing team spirit to create awareness raising messages in a playful way to the youngest!].

Isabelle FALQUE-PIERROTIN

Moderator of the International Working Group on Digital Education

[9] Study on "The management of competitions for young people on protection of personal data" – September 2015

Annex

Report of the International Working Group Concerning Digital Education September 2017

39th Conference of the International Data Protection and Privacy Commissioners' in Hong Kong

Name of Office: The Office of the Privacy Commissioner of Canada

Results of the Survey on Educational Service Platforms

INTRODUCTION

Learning platforms are integrated sets of interactive online services that provide teachers, learners, parents and others involved in education with information, tools and resources to support and enhance educational delivery and management.

The precise nature and form of these technologies varies from school to school, most often involving the use of management information systems, virtual learning environments, communications technologies and other information and resource sharing technologies. In many schools these technologies are integrated into shared online systems and environments referred to as 'learning platforms' that allow teaching staff, learners and parents to access learning resources, communicate and collaborate with each other, and enable schools to monitor, assess and report on learner progress (including *learning analytics*).

This survey intended to identity the policies, safeguards and/or provisions put in place with regards to students' personal data by both data protection authorities and educational authorities. The survey speaks to work committed by the International Working Group on Digital Education (DEWG) in the 2016-17 common action plan presented and endorsed at the closed session of the 38th International Conference of Marrakech. Among other goals, the action plan seeks to examine the question of development, and widespread use on the part of educators and their students, of eLearning platforms and online services and applications dedicated to the education community, developed and made available online, usually free of charge, by private service-providers, and raising (as in another sectors) issues with regard to collection of students' personal data, from minors in particular.

SUMMARY OF SURVEY RESULTS

In July 2017, staff of the Commission nationale de l'informatiques et des libertés (CNIL) and the Office of the Privacy Commissioner of Canada (OPC) distributed a survey to all ICDPPC members to collect information about their experiences with educational service platforms.

We received responses from 33 authorities from North America, Europe, and Asia. A summary of these responses can be found below.

1) Overview of Prevalence in Jurisdictions

Of the 33 ICDPPC members that responded to the survey, 28 stated that they had jurisdiction in this area. Of the members with jurisdiction, 18 respondents answered that they had received complaints regarding educational service platforms. When asked who the complaints were directed against, 12 authorities indicated that the complaints were directed towards the School Board or Ministry of Education, 4 members specified that the complaints were against the platform providers, and 2 did not provide details.

Although some respondents could not provide concrete numbers regarding the amount of complaints received by their offices, of those that did provide figures, 28 complaints had been received thus far.

2) Public Reactions and Engagement

When asked about the public reaction to educational service platforms, 15 members noted that they were aware of a reaction from the general public, teachers, parents or other stakeholders regarding the collection, maintenance and use or tracking of students' online personal information. Of those that indicated they were aware of public reactions, 13 of these members provided links to relevant newspaper articles, blog posts, or other related materials on this issue. The list of links provided can be found in Appendix A, while highlights from more detailed answers are included below.

> *Engagement with Government*: Some respondents provided detailed answers regarding their involvement with government to express their concerns in this area and echo the comments made by their stakeholders. For instance, one respondent (CNIL) highlighted their call for a framework for digital services in education.[1] Another respondent (ICO for UK) communicated that they have been engaged with regional governments responsible for education to help prepare for the new GDPR law.
>
> *Engagement with Teacher Associations:* One respondent, the Alberta OIPC, noted that they heard concerns from teachers and school administrators through a workshop co-hosted by their office, the research from the eQuality Project, and the Alberta Teachers' Association. They further noted the Alberta Teachers Association published a series of

[1] https://www.cnil.fr/fr/la-cnil-appelle-un-encadrement-des-services-numeriques-dans-leducation
https://cdn2.nextinpact.com/medias/courrier-men-12-avril-2017.pdf

articles relating to "Assessment in the Era of Big Data" in the summer 2017 issue of its magazine.[2]

Engagement with Advocacy Groups: The ICO for the UK noted that Big Brother Watch (an advocacy group) published a report raising concerns regarding classroom management software and excessive surveillance of student online activity. They reported concerns that schools implementing Bring Your Own Device (BYOD) will inadvertently be monitoring pupils' online activity both in and out of school.[3]

3) Questions about Compliance

When asked whether they have received questions or requests for advice regarding the compliance of these education platforms with their data protection regulation, 21 members responded that they have.

It was further noted that these requests have been received from individual parents, parent/guardian associations, teachers' associations, and service providers.

Questions surrounded the recording of absences in google docs (Suisse); providing interpretations about the use of Skype in distance learning (Czech); requirements for consent and notice with parents (Czech); and visibility of personal data on the platform (Dutch). Those with (Lithuania) and without (INFOEM) jurisdiction in this area, have been asked about the use of targeted advertising on the platform.

Members noted that they have received requests regarding compliance of platforms such as Microsoft Office 365, myschool (https://myschool.sch.gr/), Apple School, and G-suite for education. Additionally, one respondent (Thüringer Landesbeauftragfter für den Datenschutz und die Informationsfreiheit - TLfDI) noted they have been asked in the past to recommend products that meet data protection requirements. They further noted that German data protection authorities are currently examining the admissibility of the use of MS-Office 365 for teaching purposes and are in contact with Microsoft.

Several respondents referenced work being done to provide those requesting information with adequate information on compliance and data protection requirements. This includes: guidance (Finland), publication of an orientation paper on online learning platforms (Philippines)[4], and assessment tools for teachers to evaluate privacy risks (Ontario).

4) Type of Information Collected on Educational Service Platforms

A list of the information collected by platforms, and the number of respondents that reported such collection can be found in Table 1 (p.4).

[2] https://www.teachers.ab.ca/Publications/ATA%20Magazine/Volume-97-2016-17/Number-4/Pages/index.aspx

[3] https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/11/Classroom-Management-Software-Another-Brick-in-the-Wall.pdf

[4] State-Commissioner for Data Protection and Freedom of Information Rhineland-Palatinate (DPA Rhineland-Palatinate**)** https://s.rlp.de/ohlernpf

Members specified other information collected included: parent login information, 3rd party cookie data, browser and device ID (Ontario), as well as civil status data /identification data, role (student/teacher), connection data, and location data (CNIL).

One respondent (Lithuania) described a popular platform that collected information regarding injuries during the education process, information if a student lives in a hostel or a school, orphanage, information on meals, health information, and data of students with special needs.

Information Collected	# of Respondents Reporting Collection
Name	18
Email, phone number	16
Login information	16
Age	14
Date and place of birth	13
Grade	13
Assessment of skills	12
Attendance	12
Identification number	12
Other	11
We do not have this information	10
Photo	9
Address	9
Punctuality	8
Connection time (for how long)	5
Number of questions asked during class	2
Number of interruptions during class	2
Time spent on task	2
Income level of family	2
Number of siblings	2
Social media monitoring	1

Table 1

5) <u>Notice and Consent</u>

When asked whether parents were informed about the collection, use and disclosure of students' personal information in relation to educational service platforms, only 1 member answered no. The majority of members (18) stated that the information was unavailable/unknown, while 12 members responded that parents were informed.

When asked if consent was obtained for the collection, use, and disclosure of student's personal information in relation to these services; 6 authorities answered that consent is not obtained, 13 authorities answered consent was obtained, and 14 authorities stated the information was not available/unknown.

Many of the comments specified that the response varied, depending on the platform and the services provided through the platform.

Responses referenced the measures that were taken to inform parents, such as the use of permission sheets (DPA Rhineland-Palatinate) and declarations of consent (Bulgaria). The Alberta OIPC noted that the school board provides template forms to teachers to customize depending on the characteristics of the app, and these forms include a link to the Terms of Use of the platform. Similarly, the Hellenic DPA noted that parents are informed by schools and the website.

<u>Obtaining Consent</u>: While 5 respondents stated that consent was obtained through implied consent to the services upon registration to the platform, 4 respondents indicated there was opt-in through the child, and 8 respondents stated there is opt-in through the parent.

One respondent (TLfDI) noted that this depended on the level of awareness of the student, and the parent would consent if the student could not. Several respondents noted that the teachers can opt-in on behalf of the student as well.

When asked whether there is an opt-out function for the parent or child, 18 members responded that this information was not available/unknown, 7 members stated there were no opt-out functions, 6 responded that there were opt-out functions for the parent, and 4 answered that there were opt-out functions for the child.

One respondent (ICO for the UK) stated that there was a ‘soft opt-in’ method was used by schools, by sending a letter home to parents allowing the child/family to decide not to participate. Over and above these opt-out functions, another respondent (Ontario OIPC) communicated that many platforms provide teachers with administrative rights to create and delete student profiles, and to honour students’ opt-out requests

Alternatives: Respondents were asked what is the legal basis for the processing of data necessary for the performance of tasks to be carried out, if consent is not obtained. Of those surveyed; 15 members stated that official rules or provisions were the legal basis, 3 members stated preliminary oversight by DPA, 2 were unavailable or unknown, and the remainder did not provide a response.

Several respondents highlighted that consent is not the only available legal basis for processing, and one member (ICO for the UK) noted that a broader question of whether consent is freely given in this context should be posed as there may be no alternatives to the platform.

Age of Consent: When asked whether there is an age restriction in the member’s jurisdiction, 19 members responded no, 11 members answered yes, and the remaining responses were not available/unknown.

Of the 11 members that responded yes, 7 members stated the age of consent was 18 years old. One respondent (Slovenia) noted that parent’s consent was needed for youth under the age of 18, but in some contexts children can give valid consent at the age of 15. Other respondents put forward 14 (Catalan) and 16 (Dutch) as the ages of consent in their respective jurisdictions.

The CNIL noted the right to erasure can be exercised by a person during his minority or once he has become an adult, without any limitation of duration for the information collection when an individual was a minor (under 18 years old).

When asked if these ages differ in an educational context, 2 authorities responded that the information was not available/unknown, 23 stated there was no difference, 4 stated yes, and the remaining surveys were left blank.

6) Collection, Use and Disclosure

Table 2 (p.6) contains the breakdown of responses from authorities when asked about the stated purposes for collection, use and disclosure on educational service platforms.
Many stated this information was unknown or varied depending on the platform and the role of the user.

Other purposes that were raised included: Feedback channel about the teacher´s performance (Finland); information for parents (Bulgaria & Alberta); reinforce positive behaviour and encourage class participation (Alberta); record participation (Alberta); reduction of bureaucracy (Hellenic); maximization of public administration effectiveness (Hellenic DPA & Lithuania); enhancement of transparency in public administration (Hellenic DPA); and successful identification of users (Lithuania).

Stated Purposes for Collection, Use and Disclosure	# of Respondents Reporting Purpose
Assessment and report on learner progress (i.e. learning analytics)	14
Statistical and scientific research purposes	7
Improvement of the technical services of the platform	10
Pedagogical follow-up of the student	16
Targeted advertising	2

Table 2

One respondent (Nova Scotia OIPC) referenced a privacy impact assessment that addressed the collection, use and disclosure of the personal information of the educators.[5]

7) Data Minimization

When asked if there is an effort made on the part of the app developers to limit the amount of personal information being collected to accomplish the specified purposes; 2 authorities responded no, 9 authorities responded yes, 19 authorities responded that the information was not available/unknown, and the remainder did not respond.

Several respondents noted that this varied depending on the platform, and one respondent (ICO for the UK) in particular expressed that this would partly be determined by whether the app developer is aware of data minimisation as an important element of compliance. Others highlighted the legislative requirement that only information necessary, as specified in relevant educational legislation, can be collected (Hellenic DPA).

In one jurisdiction (Alberta), the authority raised the strategy employed in schools that students are encouraged to use a pseudonym when setting up a username for login purposes.

8) Secondary Use

When asked whether personal information collected by service providers is used for non-education purposes or third-party use such as targeted advertising, 12 members replied no, 3 members stated yes, 14 members answered that the information was not available/unknown, and the remainder did not respond.

Several respondents communicated that this practice varied depending on the platform, and secondary use is not permitted unless consent is obtained. One respondent (Slovenia) explained that other secondary uses would constitute illegal processing in their jurisdiction. Another respondent (CNIL) referenced the Gestionnaire d'accès aux resources' framework, a draft framework that provides for a proportionality check and calls for prohibition of this use for commercial purposes. One response (ICO for the UK) stated that some providers are adapting

[5] https://drive.google.com/file/d/0B7Ev_gwf02s2RG5xM1M5d3VaekU/view?usp=sharing

their services to remove ads and informing their users that information is not being collected for this purpose.[6]

Regarding their experiences with secondary use on educational service platforms, two respondents (Estonian & Lithuanian) stated they had complaints touching on this issue. Another respondent (Ontario) explained that the platforms reviewed through a sweep exercise appeared to involve the use and disclosure of student personal information when allowing students to use social login (Facebook Connect, Google+) and by allowing third-party tracking cookies to be placed in users' browsers. Another participant in the sweep exercise (Canada) noted that this data flow needs to be examined further.

When asked whether there was a way for students or parents to refuse the secondary use, 2 authorities responded no, 7 authorities responded yes, 12 authorities responded that the information was not available/unknown, and the remainder did not respond. In response to this question, one member (CNIL) raised the point that the individual has the right to oppose, for legitimate reasons, their data being processed.

9) Bring Your Own Device (BYOD)

When asked whether they have seen issues of students using personal devices to access the educational services apps; 7 members responded no, 5 members responded yes, 17 members responded that the information was not available/unknown, and the remainder did not respond.

Respondents noted that the platform is often times accessible from the home and through personal tablets.

One respondent (Finland) noted that they will be drafting guidelines jointly with other authorities on this, and another member (ICO for the UK) noted they have produced guidance on this topic.

One respondent (CNIL) referred to the Education Code for their jurisdiction that states the use of a mobile phone by a student is forbidden in nursery schools, elementary schools and colleges during any teaching activity. Although, they did note that there is no express prohibition in high schools except in accordance with rules and procedure.

10) Data Localisation

When asked if the storage/hosting location of the student's information is restricted to the jurisdiction, 7 members responded yes, 11 members responded no, 12 members responded that the information was not available/unknown; and the remainder did not respond.

Respondents commented that this varied depending on the platform, and one member (ICO for the UK) proposed that guidance from government would help raise awareness amongst schools regarding the risks of storing information abroad.

[6] https://edu.google.com/trust/#are-there-ads-in-google-apps-of-education

One respondent (CNIL) noted that while accommodation in France or Europe is favored, a country offering an equivalent level of protection is adequate.

11) Retention and Disposal

When asked what retention and disposal policies organizations have in place (i.e. destruction upon graduation), 8 members responded that they were unaware of any.

Many of the respondents referenced the need to adhere to the authorities' respective legislation and other local laws regarding retention and disposal. In the case of one respondent (DPA Rhineland-Palatinate) power is given to the schools to define deletion schedules for the data.

Three respondents (Valais, & Philippines, Suisse) noted that there are currently no policies in place.

One respondent noted there are several circumstances for the deletion of data. Specifically:

1. If the consent is revoked (TLfDI);
2. Observance of possible retention periods in the jurisdiction;
3. If the data is no longer needed for the task, such as the end of a school year (Morocco, Bulgaria, TLfDI);
4. User accounts of pupils and teachers should be deleted after leaving the school or after revocation of the consent (Czech, Mauritius, and TLfDI); and
5. Log data should be deleted after a maximum of 10 days (TLfDI).

One respondent (CNIL) noted personal data processed in this context shall be updated at the beginning of each school year or university year, and deleted within three months provided that the person concerned is no longer required to hold an account.

12) Safeguards

When asked what safeguards schools and app developers have in place for protecting student information; 7 authorities stated that the information was not available/unknown, and 4 authorities did not provide a response. The answers from those that responded included:

- Use of secure websites (https instead of http);
- Use of password protection to access the platform with a two-factor-authentication for administrative teacher accounts;
- Not storing authentication data in clear text;
- Use of encryption on the data-transfer between server and user/client;
- Restriction of access to user data according to role (student, parent, teacher);
- Disconnection of system not used for 45min;
- Appropriate monitoring and review of procedures;
- Train staff regularly on procedures;
- Maintain a secure premises; and
- Maintain backup copies and regular logging.

Many respondents referenced the safeguarding requirements found in their respective legislation, children's laws, and guidance.[7]

13) Access to Information

When asked whether students, or their parents, may obtain access to the personal information collected by companies, 16 members stated yes, 2 members stated no, 12 members stated that the information was not available/unknown, and the remainder did not respond.

Several respondents noted that while there is a right to access, it is unclear how this works in practice.

14) Procurement of Educational Service Platforms

When asked whether these systems are being chosen and implemented through schools or school boards with commercial contracts, 5 authorities responded no, 9 authorities responded yes,18 authorities responded that the information was not available/unknown, and the remainder did not respond.

When asked whether these contracts contain provisions that adequately protect students' personal information such as prohibition of selling of student data and providing access to parents and students; 1 member responded no, 6 members responded yes, 16 members responded that the information was not available/unknown, and the remainder did not answer.

One respondent (ICO for the UK) noted that while these provisions are not in the contract per se, they are aware that some app developers have adapted their products and privacy notices to inform users about use of behavioural targeting.

One respondent (Slovenia) explained that in their jurisdiction, the rules regulating contractual processing apply and are mostly implemented adequately. In this context, data processors may perform individual tasks associated with processing of personal data within the scope of the client's authorisations, and may not process personal data for any other purpose. They further noted that the contract must also contain an agreement on the procedures and measures pursuant to Article 24 of the *Personal Data Protection Act* and further detailed in Art. 11.[8]

15) The Role of the Ministry of Education

When asked whether the Ministry of Education provided some guidance and recommendations regarding the use of these platforms, 3 members stated no, 10 members answered yes, 17 members responded that the information was not available/unknown, and the remainder did not respond.

Several respondents referenced the guidance materials put out by their respective ministries of education in the context of educational service platforms (Catalan,[9] Wales[10], and Northern

[7] https://s.rlp.de/ohlernpf

[8] https://www.ip-rs.si/en/legislation/zakon-o-varstvu-osebnih-podatkov/.

[9] http://ensenyament.gencat.cat/ca/departament/publicacions/colleccions/tac/moodle/
http://ateneu.xtec.cat/wikiform/wikiexport/cmd/tac/moodle2/b1_eva/index

Ireland[11]). One respondent (INAI - Mexico) highlighted the work being done by their Ministry of Education in terms of training and workshops. While another (Czech) referenced a strategy being put forward by their Ministry of Education for digital education to respond to the ongoing development of digital technologies, and anticipate the gradual integration of modern technologies into education.

Several respondents noted the tools and checklists that have been developed and used by these bodies. For instance, one respondent (Ontario) noted the Ministry of Education receives advice from a committee that has developed assessment criteria and resources in this area.[12] While another respondent (ICO for the UK) noted they collaborated with the Ministry to develop a self-certification checklist.[13]

16) The Role of Data Protection Authorities

When asked how data protection authorities assist the teachers, the schools and school boards, and the commercial entities; many respondents provided links to their offices resources. The links to websites and resources can be found in Appendix B.

Respondents referenced their education and awareness campaigns (Philippines and Ontario), as well as workshops, lectures, and training geared towards educators and students (Finland, Hellenic DPA, Alberta, Mauritius, National Institute for Transparency, Access to Information and Personal Data Protection. ICO for the UK, and the CNIL)

Several respondents noted they have provided and/or are willing to provide advice in this area with school boards, educators, students and parents (Dutch and Alberta). One respondent (ICO for the UK) noted an initiative whereby they run a helpline (phone, e-channels) which individuals and organizations can use to obtain advice.

Respondents referenced the establishment of committees and partnerships. For instance, one member (Finland) communicated the establishment of a permanent data protection steering board for the education sector. Respondents also note collaborations with teachers' associations, unions and ministries of education to develop resources and assessment tools for teachers and school administrators (INFOEM and INAI Mexico, Alberta, ICO for the UK, and CNIL, National Institute for Transparency, Access to Information and Personal Data Protection), supporting academic and non for profit research in this area (Alberta), and working with those that set the curriculum (Alberta[14]).

[10] http://gov.wales/docs/dcells/publications/160817-security-guidance-en.pd

[11] https://www.education-ni.gov.uk/articles/education-safe-and-effective-practices
The Digital Schools Awards build in privacy to embedding of technology:
http://www.northernirelandchamber.com/member-news/9-new-primary-schools-in-northern-ireland-recognised-with-digital-schools-of-distinction-award-2/
The General Teaching Council NI sets the standards for teachers -
http://www.gtcni.org.uk/index.cfm/area/information/page/profstandard
support plans for governors:http://www.eani.org.uk/_resources/assets/attachment/full/0/47625.pdf

[12] https://www.osapac.ca/dlr

[13] https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

[14] https://www.oipc.ab.ca/media/813627/Speech_Alberta_Education_Curriculum_Working_Groups_May2017.pdf

ANALYSIS

The responses derived from the survey amongst ICDPPC members on educational service platforms provides a good starting point for work in this area. The comments received have demonstrated that many data protection authorities have jurisdiction over educational service platforms, and are being called upon to investigate and provide advice on the platforms' practices. Given the prevalence of complaints and demands for advice, further work is needed to support policy efforts in this domain.

The survey found that the data being collected, used and disclosed on these platforms is diverse and of a high volume. While many of the purposes for collection have clear linkages to the educational context in which these platforms operate, the responses indicate that data protection authorities would benefit from additional research into secondary uses, such as targeted advertising.

The survey identified different opt-in/opt-out mechanisms and frameworks for consent; it was made clear that this differs depending upon the platform and the legislative requirements of each jurisdiction.

The report highlights interesting considerations for authorities developing retention and disposal criteria in the context of educational service platforms, over and above the general retention schedules found in respective privacy legislations. Those that participated in the survey also raised several robust safeguarding measures that should be taken into account by those holding and processing student data on these platforms. These findings, as well as the guidance put forward by the respondents, form a useful collection of data and resources for ICDPPC members.

RECOMMENDATIONS

- The survey results should be reported at the 39th Conference of the International Data Protection and Privacy Commissioners' in Hong Kong for consideration of all members of the ICDPPC.
- Members should be encouraged to continue to report the survey responses to the Digital Education Work Group secretariat, who will add the responses to the survey database, and make these available to members upon request for future research purposes.
- In order to determine next steps, the Digital Education Working Group should establish a taskforce on educational service applications with data protection authorities that have extensive experience in this area.
- The Digital Education Working Group or its taskforce should determine areas where further research should be conducted based on the needs identified in the survey.
- In order to coordinate efforts, and leverage resources, the results of the survey should be observed by ICDPPC members as they undertake work in their respective jurisdictions.

APPENDIX A

http://epep.educanet2.ch/classe.haeni/classe_Haeni/p.29.html;

http://epep.educanet2.ch/classe.valley/Classe_Oiselier_GVT/Mes_albums/Pages/Nous_en_classe.html#4;

http://epep.educanet2.ch/classe.kury/Classe_A._Kury/Bienvenue.html;

http://epep.educanet2.ch/classe.ribeaud/Classe_V.Ribeaud/Bienvenue.html;

https://www.rtlnieuws.nl/nieuws/binnenland/gegevens-leerling-niet-zomaar-naar-uitgever

http://www.alfavita.gr/arthron/ypoyrgeio-paideias/o-diofantos-minyei-proto-thema-gia-myschool; http://www.protothema.gr/greece/article/698675/huma-sto-idernet-ta-stoiheia-hiliadon-paidion-kai-nipion/;

http://www.newsbeast.gr/greece/ekpaideusi/arthro/653026/prosfugi-tis-olme-kata-tou-myschool;

http://www.infoem.org.mx/doc/avisosDePrivacidad/CAPACITACIONES_Y_PLATICAS_INFORMATIVAS.pdf;

http://www.deutschlandfunk.de/datenschutz-in-der-schule-orientierungshilfe-fuer.680.de.html?dram:article_id=350587; http://www.cndp.ma/fr/actualite/271-act-cndp-28-01-2015.html;

http://ifaininos.ifai.org.mx/; “Procupeques” programme of the Federal District Attorney's Office

http://www.procupeques.gob.mx/recomendaciones.html; "Ciberseguridad México 2017" campaign to bring information to schools so that students avoid cyber attacks such as identity theft:

https://www.gob.mx/policiafederal/articulos/policia-federal-impulsa-la-campana-ciberseguridad-mexico-2017#acciones ; Decalogue for Safe Browsing on the Net, @prende.mx, available at:

http://www.aprenderecursos.sep.gob.mx/pdf/decalogo_navegar_seguro.pdf; y Educational multimedia pack “Las diez claves” (To use the Internet safely): http://www.pantallasamigas.net/recursos-educativos-materiales-didacticos/cd-las-diez-claves/index.htm;

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/statement-in-response-to-new-snapchat-location-feature/; http://www.letudiant.fr/educpros/

http://www.snes.edu/Numerique-le-SNES-FSU-s-adresse-a-la-CNIL-et-au-Ministere.html;

http://www.snes.edu/IMG/pdf/2017-06-15_v2_lettre_a_mme_moreau-reglementation_concernant_le_numerique.pdf;

http://www.cafepedagogique.net/lexpresso/Pages/2017/05/23052017Article636311196795121014.aspx

APPENDIX B

Canada:
Resources and Research https://www.priv.gc.ca/en/privacy-topics/privacy-and-kids/02_05_d_62_tips/
Youth Site – www.youthprivacy.ca

Catalan:
http://apdcat.gencat.cat/en/contacte/index.html
http://apdcat.gencat.cat/web/.content/03-documentacio/materials_jornades_i_congressos/documents/2890.pdf

Czech:
https://www.uoou.cz/odbornici-uradu-prednaseli-na-gymnaziich-a-nbsp-krajskych-uradech/d-22707
https://www.uoou.cz/11-rocnik-souteze-moje-soukromi-nekoukat-nestourat-quot-ma-sve-viteze/d-23879
(Educational video) http://www.ceskatelevize.cz/ivysilani/1096056775-pomahejme-si/21154311505/

Dutch: https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/onderwijs

France:
Informations et FAQ- https://www.cnil.fr/cnil-direct?visiteur=pro
Rubrique Education- https://www.cnil.fr/cnil-direct/thematique/80?visiteur=pro
https://www.educnum.fr/fr/la-cnil-part-la-rencontre-des-enseignants-pour-les-former-la-protection-des-donnees-0

Hellenic DPA:
www.dpa.gr
Education and Children site:
http://www.dpa.gr/portal/page?_pageid=33,97846&_dad=portal&_schema=PORTAL

Morocco:
Guidelines for website compliance http://www.cndp.ma/en/dossiers/m-conformite-sites-web.html
Convention with the Ministry of National Education. http://www.cndp.ma/fr/actualite/271-act-cndp-28-01-2015.html

Mexico - National Institute for Transparency, Access to Information and Personal Data Protection
www.inai.org.mx
Guide to comply with the principles and duties of the Federal Law on the Protection of Personal Data held by Private Parties:
http://inicio.inai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pd f
Manual on personal data security for MSMEs and small organizations-
http://inicio.inai.org.mx/DocumentosdeInteres/Manual_Seguridad_Mipymes(Julio2015).pdf
Guide to implement a Personal Data Security Management System -
http://inicio.inai.org.mx/DocumentosdeInteres/Guía_Implementación_SGSDP(Junio2015).pdf

Ontario: https://www.ipc.on.ca/teachers-must-consider-privacy-before-using-online-services/

Philippines:
www.privacy.gov.ph

Rhineland-Palatinate:
Orientation-paper - https://s.rlp.de/ohlernpf

Suisse:
https://www.ppdt-june.ch/fr/Documentation/Index/Ecoles-et-formations/Ecoles-et-formations.html

Sweden:
(Reports) http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2017/06/sou-201749/
http://www.regeringen.se/49c6b6/contentassets/56e701d354824bcb9826ea0839ab28f3/sa-starker-vi-den-personliga-integriteten-sou-2017-52.pdf

Thüringer Landesbeauftragfter für den Datenschutz und die Informationsfreiheit (TlfDI):
Guidance to the DPAs for online learning platforms in school teaching
https://www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/oh-lernplattformen.pdf

United Kingdom:
Education sector resources page - https://ico.org.uk/for-organisations/education/
Information Rights factsheets for new school governors-
http://www.governorswales.org.uk/publications/2015/09/29/data-protection-act-1998/
GLOW- https://connect.glowscotland.org.uk/
Privacy Impact Assessment - https://glowconnect.files.wordpress.com/2015/06/glow-privacy-impact-assessment-draft-may-2015.pdf