



**GPA**

Global Privacy Assembly

# Digital Education Working Group

Report – October 2020 (final 20201013)

Chair Authority: CNIL France

## Table of Contents:

Executive Summary	.....	p. 3
Introduction	.....	p. 5
Working group activities	.....	p. 6
Forward looking plan 2020-2021	.....	p. 11
Conclusion	.....	p. 13
Annexes (4)	.....	p. 14

1. DEWG 2020 Summary report survey evaluating impact of the Data Protection Competency Framework

2. DEWG Survey information – Summary report of 25 August 2020 on:

The legal frameworks and practices of data protection authorities regarding the exercise of the rights of minors – Section 1

Putting into perspectives other international initiatives on the issue of minor's rights - section 2

3. DEWG 2020 Survey report: results of the questionnaire regarding implementation of the Resolution of e-learning platforms.

4. DEWG CIRCABC platform Folder tree

## Executive Summary

The Digital Education Working Group (DEWG) has been tasked with a number of actions coming out of the Policy Strategy and a number of initial objectives in place for several years deriving from the Resolution on Digital Education for all attributed to the DEWG. As a consequence, the scope of activities is quite large and reflective of the different responsibilities and roles of the stakeholders impacting challenging annual tasks and activities by our DEWG, and including the monitoring of the work of Data Protection and Privacy enforcement authorities as well as of other International organizations to join forces together and reach consistent objectives.

There are four main topics that the DEWG has been working on:

**As the first topic**, the DEWG produced an overview of successful integration of data protection topics and competencies by age group in the school curriculum. The DEWG has been mapping over recent years progress made in integrating the international Data Protection Competency Framework (adopted in 2016 by the ICDPPC) in curricula. The process of integrating these key data protection competencies into national or regional curriculum may vary according to jurisdictions on the method and timely manner, but following a multidisciplinary approach as recommended. This year's enquiry was aimed at mapping the successful impact of the Competency Framework on data protection knowledge and skills acquisitions in primary and secondary schools, as well as to identify whether any other tools or strategies are needed to enrich the school programmes and in-service and continuous training sessions of educators in the data protection area.

**The second topic** was awareness raising on the exercise of digital rights by children, noting it is a core part of the DEWG's mandate. The final objective of this work is a future guidance document to inform children of their rights and how to exercise them, but first there was a need to identify legal frameworks.

In brief, the results of the study report on legal frameworks based on 46 responding countries, Section I, show that there are some provisions for children to exercise their privacy rights, but there is not as much clarity around who is able to exercise those rights – for example children, parents on their behalf, bearing in mind notions of digital maturity and the capacity of children.

Section II of the report on international perspectives is monitoring specific national consultations (ICO, DPC, and CNIL) and major international initiatives in relation to the exercise of children's rights.

Further explorations arising from the 2019 questionnaire to DPAs were meant to take stock of initiatives and emerging good practices of related appropriate information systems to raise awareness of children and/ or the legal representatives, according to the age and the level of maturity to get them to exercise or to resort to remedies to access counselling and reporting mechanisms and assistance to activate their rights given development of capacity in children's age ranges. Findings from the DPAs' responses resulted in the obvious absence on DPA websites of any related specific child-friendly guidance released on existing privacy rights granted to them<sup>1</sup>. As a consequence, the objective to build on good practices as to information process in place to possibly lead to joint recommendations couldn't be met and should be considered in the 2020-2021 Work plan.

Contributing to this work, CNIL has recently explored and initiated an overview of a sample panel of websites providing content specific to kids and youth with prominently sign-posted information

---

<sup>1</sup> As conclusions gathered from the 2019 survey

specific to minors and age appropriate children or directed at parents that could be extended at next year's work plan highlights to share good practices among DPA members.

**The third focus** was developed in furtherance of the adoption of the 2018 [Resolution on e-learning platforms](#) (Brussels). The DEWG produced in Tirana (ICDPPC, 2019) a first Report regarding the Implementation of the Resolution on e-Learning Platforms<sup>2</sup> which highlighted initial progress by data protection authorities on their engagement with government and school authorities, development of useful resources, and outreach activities and suggested follow up activities. It was decided to continue to track the progress of interactions with relevant stakeholders in the field of education and the industry over a longer period of time –not limited to one single year - to monitor success and impact in the adoption of emerging Codes of Practice, lessons learned, and contribute to an understanding of why some initiatives may not have been adopted in some jurisdictions. Therefore, the questionnaire was reissued in 2019-2020 and rolled out under the specific situation of the COVID 19 crisis which has led to online educational continuity across all the countries. This has been obviously posing technology and privacy-related challenges and reinvigorated the need to produce security and data privacy guidance for schools authorities and other stakeholders, pointing out the most operational and compliant way to implement guidelines as made available in the 2018 Resolution on e-learning.

Due to the abrupt shift to distance learning in response to COVID-19, school closures have accelerated the process dramatically of digitalizing and storing at an unprecedented scale, including data about learning processes (as varied as thinking characteristics, learning trajectory, engagement score, response times, pages read, videos viewed...). This has obviously propelled the much needed dialogue of AI and learning analytics in Education to the top of the agenda of national and international debates for the time to come. No progress was registered this year in coordination with the permanent GPA Working Group on Ethics and Data Protection in Artificial Intelligence which had some flexibility to have this activity carried out at a later stage.

**The fourth focus** was referring to the update of the CIRCABC e-library with content adapted to the revised classification of key interest of DPA members. The objective was to help maintain the platform in an attractive and informative manner in furtherance of continuous sustainable efforts produced to upload new resources and materials. The CNIL and the CNPD (LU) acting both as coordinators of the CIRCABC platform have been committed over the past year in a comprehensive project to update the CIRCABC platform of online resources which will be achieved by 30 September 2020 with the opening of the new and revised library offering access to updated quality documents. A new governance arrangement has also been discussed to maintain the back-up of the interest group established as of 2014 with the EU Commission hosting the Platform for both EU and non-EU DPAs.

## Introduction

*List of Digital Education Working Group (DEWG) members*

Lead: FR - Chair: CNIL, France - Marie-Laure DENIS & Pascale RAULIN-SERRIER

---

<sup>2</sup> The report produced in English and in French was circulated to the closed session in 2019 and can be made available on request to Melissa Goncalves at the OPC and Pascale Serrier at the DEWG Secretariat

Other delegations: Albania, Belgium, Bosnia and Herzegovina, Bulgaria, Catalonia, Croatia, Cyprus, Czech Republic, EDPS, Estonia, Finland, DE (and regional DPAs- LfDI), Georgia, Gibraltar, Greece, Hungary, Ireland, Island, Italy, Jersey, Latvia, Lithuania, Luxembourg, Macedonia, FYROM, Moldova, Monaco, Norway, Poland, Portugal, Romania, Spain, Slovakia, Slovenia, Switzerland (and Swiss Cantons), UK, Council of Europe, EDPS, Burkina Faso, Gabon, Ghana, Ivory Coast, Mali, Morocco, Mauritius, Senegal, Tunisia, Cap Verde, Canada (OPC), Canada (Ontario), Canada (Québec), Canada (Alberta), USA (FTC), Columbia, Mexico, State of Mexico, Uruguay, Hong Kong, Korea, Macao, Singapore, the Philippines, New Zealand, Australia, Australia (Victorian DPA), Israel.

This year, GPA members of the DEWG have been invited to express their views and participate in several follow-up surveys of ongoing actions and explore new fields of cooperation set in the 2019-2020 work plan program.

Core issues of the DEWG are to protect children's rights in the digital environment; clarify and facilitate the exercise of children's rights in the digital age where there is an interest in children's rights; integrating data protection topics in school curricula to train teachers, students and empower more resilient children; monitor e-learning platforms in schools facing aggregation and integration of data, leading to an unprecedented scope of inferred information about learners; survey challenging technologies used to capture, store and make sense of learner data and analytics that can also make predictions about future performance of individuals and generate faulty, biased or discriminatory conclusions and indeed have carried significant consequences for learners.

The DEWG, in its leading role, has already proposed and adopted 3 key resolutions, an international Data Protection Competency Framework for school students intended to help educators, has been sharing resources on an e-library platform as well as conducting international benchmarks in our area of data protection, producing studies on the training needs of students and teachers in the digital universe, a Guide on conducting national competitions with pupils and students on our topics and most recently mapping the legal frameworks and the state of practices concerning the exercise of the rights of minors.

As a matter of fact, the DEWG is aware that authorities this year have been facing simultaneous competing priorities. Recognizing it was hard work to mark effective progress in the wider regulatory landscape over this specific year, it has to be considered as satisfactory to have addressed the analysis of contributions of sometimes limited panels of DPAs which nevertheless allowed to draw some conclusions on certain tendencies regarding issues at a broad cross-sectorial country level.

As Chair, I am happy to convey this message to GPA to have valuable efforts of our DPAs community recognised especially in 2020. And I would like to also thank the sustained efforts and pro-active collaboration of co-leaders having supported CNIL's staff in conducting some activities on behalf of the DEWG, namely the OPC of Canada and the CNPD of Luxembourg.

## Working Group Activities

### **Action 1: Providing an overview on the successful integration of data protection topics in curricula**

Further to the annual investigations by the DEWG on this topic, the survey conducted until 15 July, 2020 had a dual purpose and aimed to explore on the one hand, whether progress had been made in curricula and school programs with the objective to acquire competences on data protection, whether the [international Data Protection Competency Framework for school students](#) has played its role as a useful guide for teachers from around the world in primary as in secondary schools, and if it would be worth enriching it or having it evolved, if so, how. And on the other hand, the DEWG raised further questions on whether other strategies or avenues would be considered relevant to improve the effectiveness of education in the data protection area.

The 2020 in-country evaluation of the implementation in curricula, school programs and training of educators of the [2016 Resolution for the adoption of the international data protection Competency Framework in Privacy Education](#) accounted for 16 authorities' answers. In term of views expressed, much support has been credited to the Competency Framework as a useful tool to be given attention as a starting point for discussions with educational authorities and according to the jurisdictions to be included as a concrete component in digital literacy curricula topic as early as primary school in some countries, while others, addressed the issue during secondary education and in higher Education. As a matter of fact, data protection is never taught as a subject by itself, but integrated into wider areas of study, among which are counted computer studies/media studies/ digital education/ Health/Sexual Education or Life management / civic education.

The original document or its adapted version by age groups was used to organize popular public competition and reach young audiences, as well as for producing resources designed for teachers such as lessons plans or booklets which are also accessible by the students themselves.

Among the strategies envisioned by the DPAs in the future, the recurring ideas included developing teacher training, in particular with online tools to enhance teacher training as a top priority in the dissemination of a digital culture aimed at students. As a shared responsibility, DPAs should also strive to further raise awareness around the 2016 Resolution, promote the updating of the Framework in order for it to stay relevant and think about disseminating indicators, to measure the effectiveness of the framework.

*Cf. Annex 1. DEWG 2020 Summary report survey evaluating impact of the Data Protection Competency Framework*

### **Actions 2 & 5: Achievements in relation to awareness-raising on the direct exercise of digital rights by children themselves & monitoring major initiatives on children's rights by OECD, Council of Europe and other International Organizations**

The International Working Group on Digital Education has produced a final report on the legislative background identified applying to children and the exercise of the rights of minors. The international study report is fed with input from the first study launched in 2018, pursued in 2019, on children's rights in the digital environment analysing specific legal frameworks applying to children in their respective countries, in order to identify their level of autonomy in exercising their own data rights.

*Cf. Annex 2. Survey information - Summary report of 25 August 2020 on the legal frameworks and practices of data protection authorities regarding the exercise of the rights of minors (section 1) and putting into perspective other international initiatives on the issue of minors' rights (section 2)*

The synthesis of 46 authorities' answers revealed that recent evolutions in the European and international legal framework tend to give children a growing capacity to exercise their rights. This dynamic is fuelled by the interpretation of the wording of data protection legislation and the Convention on the Rights of the Child (CRC).

The final objective is to have clear guidelines incorporated into a future guidance document to inform children of their rights and how to exercise them, but first there was a need to identify legal frameworks as a valuable overview. If there has been identified some provisions for children to exercise their privacy rights, there is however not as much clarity around who is able to exercise those rights – for example children, parents on their behalf, bearing in mind notions of digital maturity and the legal capacity of children.

To make the link with the second part of the DEWG survey conducted in 2019, the main focus was on the available information systems by DPAs intended for minors relating to the processing of their personal data, the rights they have in this regard and about the existence of mechanisms for alerts or complaints specific to minors to the APD.

Out of the survey results based on 27 DPAs responding (i.e. one third of the panel of 65 surveyed), it revealed that the authorities' websites do not offer information on the exercise of rights, nor counselling or remedies or complaint mechanisms specifically addressed to minors. In consistency with the results highlighted by the international study on legal frameworks, in the absence of a clarified doctrine on the issue, some DPAs indicated that they generally would be willing to accept online complaints (or any reporting) from minors whatever the age even if they do not have a special procedure established for minors. As a matter of fact, several DPAs specified in the survey that they were thinking on the one hand, about ways to improve and measures about counselling, advice and information in a dedicated section on their website adapted to children, or to provide tools facilitating the understanding by children and youth on how to enact and exercise their rights, and access remedies or complaints in a child-friendly way. On the other hand, some were planning to post information intended to redirect children or minors to other agencies likely to provide them with assistance (in the case of cyberbullying, for example) in order to facilitate interaction with young people.

In endeavoring to finalize the work program on this issue, the CNIL has engaged in some work that may be of relevance based on research from a sample of DPAs' websites or platforms with partnering organizations posting data protection content suitable for children and young people. The results of this overview aim to illustrate some innovative practices and approaches to develop communication means suited to the mode of expression for children on issues they may encounter on the internet or social networks.

See the **DEWG's forward looking plan** that invites GPA members to continue feeding and polishing this overview and having proposed extending the working document to a larger eligible panel of relevant websites for young people throughout 2020-2021.

**The report is also putting into perspectives on other international initiatives on the issue of minors' rights** complemented by short notes (focus) on : the content of the ICO Age Appropriate Design Code (AADC) of practice for online services, the outcome of the public consultation conducted by the DPC

of Ireland on the processing of children's personal data and the rights of children that is expected to produce guidance for the drawing up of one or more Codes of Conduct on the processing of children's personal data, the Ontario Legislation, 2020, Part X of the Child, Youth and Family Services Act, and the possible revision of the Children's Online Privacy Protection Act (COPPA) in the USA .

A brief insight has also been considered worth mentioning about the French CNIL's initiative which has started a comprehensive discussion on the rights of minors over their personal data and on the conditions under which they should be encouraged to exercise them. For this purpose, the French DPA has also been running a consultation towards various stakeholders, including parents, youths, the educational community and professionals from the digital sphere which ended in June 2020. Final outcomes will be published in late autumn.

The DEWG is further reporting on the monitoring related to major initiatives on children's rights in the digital environment under timely converging drafting processes, namely by the UN [Convention of the Rights of the Child], OECD [revision of the 2012 Recommendation on the Protection of Children Online], the Council of Europe [draft Guidelines on Children's Data Protection in an Education setting by the Convention 108 Consultative Committee], and other international Organizations like ITU-COP [The 2020 Guidelines on Child Online Protection (COP) published on 24 June 2020], ENOC network [Position Statement on "Children's Rights in the Digital Environment" adopted in September 2019 by members of the European Network of Ombudspersons for Children, UNICEF 2018 Guide on children's online privacy and freedom of expression or planned at the European Union level.

### **Focus on the UN Convention on the Rights of the Child**

The UN Committee on the Rights of the Child (CNUDE) is drafting a General Comment on children's rights in relation to the digital environment. All interested parties were invited to a first round closed in May 2019 to comment on the original concept note of the General Comment (135 submissions are available). In parallel, consultations with children across multiple countries have been undertaken to ensure that their perspectives are fully reflected in the General Comment. The UN Committee is currently preparing a first draft of the General Comment.

The DEWG has first liaised with Ms. Elizabeth Coombs, the Chair of the 'Privacy and Personality' Taskforce of the UN Special Rapporteur on the right to privacy, leading the 'privacy and children' CRC and made contact with the CRC secretariat. This has informed us that the draft general comment is intended to be published for, a second and last round of public consultations between mid-August and mid-November 2020 on the CRC website whenever available.

The DEWG is calling for the establishment of a sub-group in this area of expertise to look through the next draft of the General Comment, deliver some analysis of the draft and make suggestions to have the text supplemented in view of the next round of CRC consultation.

Supplementing the UN Convention on the Rights of the Child with due protection of digital rights in addition to the existing privacy rights is high on the international agenda of the GPA as one of the Conference's strategic missions.

### **Action 3: Implementing the Resolution on e-learning platforms**

The DEWG has been continuing to track activities to monitor progress in this key area, as well as success and impact in advancing and disseminating this 2018 key Resolution.

For this purpose, the same questionnaire as in 2019 was distributed to its DPA members in February 2020. The deadline for responses was extended to 1<sup>st</sup> July.



In the wake of the COVID-19 pandemic, countries around the globe have been called upon to redefine the way they operate in an effort to protect against the spread of the virus. Now more than ever, digital services and technologies have been relied upon since many schools have closed their doors, and shifted from in-person to online learning. While this shift has proved necessary to continue to educate students, it remained important that the privacy rights of students, teachers and parents continued to be upheld, that it could be guaranteed that the data collected was solely used for educational purposes in compliance with data protection law.<sup>3</sup>

Therefore, the work of the Global Privacy Assembly's Digital Education Working Group (DEWG) as valuable guidance to mitigate privacy risks was promoted to help educators and schools which began to consider integration of e-learning at this time and could run the risks of adopting unapproved app, website, and other resources not made for education. It was considered all the more relevant and timely to have the key privacy and security considerations of the Resolution addressed to all stakeholders including educational authorities, manufacturers of computer software, mobile applications, and web-based tools specifically provided to schools.

As a result of this year's survey, some 15 updated replies were analysed by the OPC of Canada acting as leader on this issue.

*Cf. Annex 3. DEWG 2020 Summary report – Results of the questionnaire regarding the Implementation of the Resolution on e-learning platforms*

It includes further interesting and promising detail regarding:

- The dissemination of the e-learning Resolution through DPA websites, workshops and webinars with international influence (UNESCO webinar and COE 108+ Convention Consultative Committee), which has brought more prevalence to our privacy message in the field of online education and provided an opportunity for alignment of recommendations in the EU and abroad.
- Contact that has been made with relevant government and education authorities through expert working groups. Several jurisdictions note that conversations around e-learning were sparked by school closures and reliance on distance learning during the COVID-19 pandemic.
- Resources such as online training, videos, and guides that have been developed for students and educators to raise awareness of the data protection risks and mitigation measures identified in the Resolution.
- Progress that has been made in several jurisdictions regarding the development of codes of conduct in the area of e-learning.

The ultimate goal is to establish a directory of Guidelines and Codes of practice developed by relevant actors in national or regional jurisdictions in relation to e-learning platforms.

This work aligns with the GPA's 2019-2020 Policy Strategy's first strategic priority, 'Advance Global Privacy in a Digital Age'. The sharing of information and experiences from national initiatives focused on children's privacy online and the mapping of data protection issues related to digital education supports broader work under Pillar 3, Action Item III of the Strategy which directs the GPA to: "Share

---

<sup>3</sup> Resolution on E-Learning Platforms: <https://icdppc.org/wp-content/uploads/2019/03/dewg-Resolution-adopted-20180918.pdf>  
[http://globalprivacyassembly.org/wp-content/uploads/2018/11/R solution-2018-Plateformes-dapprentissage-en-ligne\\_VD-finale-23.10.2018.pdf](http://globalprivacyassembly.org/wp-content/uploads/2018/11/R solution-2018-Plateformes-dapprentissage-en-ligne_VD-finale-23.10.2018.pdf)

information and experiences from national initiatives focused on children's privacy online and map the related data protection issues".

In relation to the 2018 core resolution, real life cases of application of AI technology relevant for ethics and data protection in school activities used for learning analytics (i.e. that are not under control over the algorithms) were planned to be collected as part of a repository. This activity will be further examined and taken appropriately forward in coordination with the permanent GPA WG on Ethics and Data Protection in AI in 2020-2021. This initiative is fully in line with Pillar #3 Action III.

#### **Action 4: Uploading new resources and materials on the CIRCABC online platform**

*Cf. Annex 4. 2020 CIRCABC new folder tree*

The CNIL and the CNPD (LU) acting both as coordinators of the CIRCABC platform are currently committed in a project to update the CIRCABC platform of online resources.

An inventory of the resources uploaded on CIRCABC has been established, a new classification with updated files produced and DPAs individually invited to review their documents and notify if they are still relevant to be transferred to the new folder tree. Until 30 September 2020, the CNPD will upload updated documents on behalf of the members. After that date, DPAs will be kindly invited to open individual accounts on the platform (appropriate procedure available) or use their dedicated account to add new online material by themselves. The DEWG intends to explore the idea of organising temporary short campaigns to mobilize DPAs during a fixed period who would be invited to download their latest and successful pedagogical resources on CIRCABC.

This initiative is fully in line with Pillar #3 Action III: Share information and experiences including ideas and success stories from the national initiatives focused on children's privacy online and helping to map the related data protection issues.



## Forward looking plan 2020-2021

In 2020-2021, the DEWG intends to focus on 3 topics in line with Capacity Building for the Conference and its Members in the GPA Conference Strategic Direction.

Based on the following considerations:

- First, the immediate and anticipated impacts of the Covid-19 crisis and mass online learning on the privacy and security of learners' data at the time when obviously many educators seem to have turned to social media / mainstream video-conferencing platforms to conduct their lessons, without a full understanding of the risks and flaws,
- Second, having teachers lacking awareness and training for quality usage instead of (or in addition to) online tools specifically developed and designed for teaching, learning or the management of education,
- Third, families were not prepared to leapfrog into a remote learning situation with regards to their children.

The DEWG finds that this is a perfect time to suggest within the 2020-2021 DEWG work plan to focus on 3 main priorities:

**Priority I- Combine relevant action items with regards to the need related to the use of digital tools and eLearning platforms in a privacy protective manner at schools and the need to support teachers, schools and parents.**

- Objective 1 – Actions towards accompanying teachers' training in relay with pedagogical tools online

In terms of effective approaches, to make an effective implementation of all the operational objectives set out in the 2018 resolution on eLearning platforms with regards to educational authorities by:

- highlighting much better preparedness of schools in distance learning at the local or national levels,
- empowering staff with basic data protection and security principles within the framework of digital literacy and privacy education as part of the in-service and continuous teacher training,
- providing teachers with extensive, updated knowledge-building and training opportunities, and curricula and evaluation criteria that enable them to implement a mixed learning approach incorporating face-to-face, and remote learning.

- Objective 2 – Actions towards accompanying parents

To support parents and offer them a broad range of insights and ideas about things they can do with their children to help them understand rights and responsibility in the digital environment.

*[in line with Pillar #3 Action III of the GPA Policy Strategy and as provided in the 2016 Resolution for the adoption of the international data protection Competency Framework in Privacy Education]*

**Rely on the timely revised CIRCABC platform providing opportunities to upload new resources and materials in relation to the above exchange of information**

*Cf. the revised folder tree of the CIRABC platform of resources*

*[in line with Pillar #3 Action III of the GPA Policy Strategy]*

## **Priority II- Consider a possible proposal for a resolution on the rights of minors**

*[in line with Pillar #3 Action III of the GPA Policy Strategy].*

i.e. with guidelines and practical recommendations, FAQs in relation to information, special focus on various design approaches to draw the attention of young people in accordance with their age and maturity on the exercise of their privacy rights, facilitation of online counselling and reporting interactions or complaint mechanisms for children directly to DPA services or to other relevant agencies.

- Objective 1:

**Pertain suggested work with regards to scanning some sites/ platforms intended for children, young people and parents that could enrich the inventory of approaches or means of communication and illustrate specifically the draft resolution on children's rights**

- Objective 2 :

**Continue the exchange on national initiatives such as drawing up of codes of Practice and mapping international guidelines concerning data processing and the exercise of children's rights in the digital age to also sustain the project of a draft resolution on this issue**

*[in line with Pillar #3 Action III of the GPA Policy Strategy].*

**Priority III- Conduct work merging respective priorities of the DEWG and the Working group on Ethics and Data Protection in Artificial Intelligence** in the perspective of the joint development of an international repository of real cases applications, with regards to data in education, the processing of school data and other traces of learning analytics

*[in line with Pillar #3 Action III of the GPA Policy Strategy]*

### **Specific short term priority**

**UN: Adoption of a joint contribution named DEWG and/or GPA members authorities concerning the United Nations General Observation at the stage of final draft text on the digital environment of children online in the UNCRC Convention, *subject to the UN calendar: to be submitted by 15 November 2020.***

<https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx>

i.e. calling for establishing a sub-group of DPA members in this area of expertise within the DEWG to conduct first analysis and drafting work for a proposal to supplement the related UN Convention.

*[in line with the GPA Policy Strategy by Supplementing the UN Convention on the Rights of the Child with due protection of digital rights in addition to the existing privacy rights].*

## Conclusion

Digital Citizenship Education is being identified as a key dimension and global component of the DEWG's international program of actions and is being placed at the core of a broad range of activities constantly evolving across issues and challenges addressing skills, learning and empowerment of children, including the exercise of their rights online.

DPA members and their educational partners have so far produced a wide range of valuable resources to support awareness-raising in digital education on the way to empowerment of children through the acquisition of competences for learning how to safely and responsibly participate in digital society. A step further needs data protection topics to be more formally included in the curricula, and taught upstream in universities of teachers' education.

The disruption brought about by the coronavirus pandemic has highlighted a lack of preparedness on the part of many school systems, both at the local and national level. It can also be a good opportunity for schools to review their approach to the use of digital technologies and to consider both whether the solutions proposed are in the best interests of the child and comply with best international practice recommended by the extensive eLearning platforms resolution.

A further aim of the collective initiative is to help foster more transparent relationships with digital technology providers in educational settings that align with relevant national, European and international standards implemented in Codes of practice.

New skills and better understanding of the whole picture of AI is required and there is a need for further cooperation between educational authorities, regulatory authorities, policy making and private sectors.

The key features of this next roadmap deserve to be supported among the GPA strategic priorities set.

## Annex 1



### SUMMARY REPORT OF RESPONSES TO THE DEWG SURVEY EVALUATING THE IMPACT OF THE COMPETENCY FRAMEWORK - July 2020

---

#### Replies from 16 DPA members (as of July 28, 2020)

17.08.2020

*This report reflects results from DEWG members' questionnaire exclusive to 2020. It does not outline the former active contributions of DPAs bringing to light results surveyed over the past years which were pointed out in previous reports.*

#### 1. Teaching data protection

In a majority of countries surveyed, data protection is taught as part of the curricula. Some countries such as Finland, France or the UK introduce the topic as early as primary school, while others, including Alberta, address the issue during secondary education. Data protection is never taught as a subject by itself, but integrated into wider areas of study, among which include computer studies/media studies/ digital education (FR, PT), Health/Sexual Education (AB, UK), or Life management / civic education (IT<sup>4</sup>, AB).

In some countries like Burkina Faso or Estonia, data protection is not formally included in the curricula, but it is taught on the initiative of individual teachers.

Data protection is also taught in universities, for example in Finland or the Philippines, or as part of vocational training in Luxembourg. Data Protection Authorities are also active stakeholders in the field of data protection education, through several types of interventions:

- By providing training/education in data protection to various audiences, including students (AB, BK, LU, GI, ALB), educators (FR, IT, ALB) and the general public (PH) through one-off awareness sessions. Some DPAs use original formats to get their points across: in Jersey, the JOIC organizes a “courtroom challenge”, where students enacted a mock trial regarding a privacy matter. Jersey also uses Young Privacy ambassadors to raise awareness among younger generations. In France, the CNIL organizes contests and hackathons to reach young audiences.

- By producing resources designed for teachers such as lessons plans (CA), booklets (MU); or accessible by the students themselves, for example websites (ME) or posters or games (FR).

Some of those events and resources are designed in partnership with other stakeholders, including educational authorities and NGOs.

#### 2. Data Protection Competency Framework and the inclusion of data protection into curricula

---

<sup>4</sup> In Italy, the Civic Education Curricula will be implemented in the coming year.

The appropriation of the Competency Framework is uneven depending on the countries. Some territories including Burkina Faso, Finland, Mexico, Albania and Alberta are in the process of including the Competency Framework to their educational curricula. This process includes discussions with the Ministry in charge of education. Some Data Protection Authorities have highlighted the fact that the Framework is extremely useful as a starting point for discussions.

Others have used the framework as a basis to develop or update educational resources and lesson plans. This is the case of Jersey, Gibraltar and the United Kingdom. In France, the framework was adapted to the different target ages and included as a part of the pedagogical resources available to educators.

In some countries, the Framework has not been appropriated by data protection authorities. In Switzerland, it is because the federal administration is not responsible for education matters. In Portugal, data protection curricula was designed before the introduction of the Framework.

3. Additional strategies that can be implemented to provide students with key data protection skills (existing or potential)

This question has been understood ambivalently by participating DPAs. Some mentioned strategies that they were implementing at the moment or that they had implemented in the past, while others described ideas or projects they might find useful in the future.

The DPAs mentioned ongoing collaboration with various public authorities and other stakeholders: In Switzerland, the FDPIC has worked with the Federal Social Security Office to launch the platform “Jeunes et Media” to promote digital education. In Finland, they have worked with the National Audiovisual Institute to organize the Safer Internet day Campaign as well as the National Game Day. They have also collaborated with national organizations to produce educational material. In the Philippines, a cooperation with the Ministry of Education has led to the implementation of the Kabataang Digital Program, which aims to promote data privacy awareness among the youth.

Among the strategies envisioned by the DPAs in the future, the recurring ideas included:

- To develop or strengthen a partnership with the Ministry of Education (BK, EE, JE, ME, PT, UK, MU, IT, ALB)
- To develop partnership with other relevant stakeholders (ME), including regional educational authorities (UK), child advocacy groups (UK) or private institutions (PH)
- To develop teacher training (FR, JE, PT, AB, LU, ME), in particular with online tools (PT)
- To develop and share tools for children (PH) and educators (ME, FR). Those tools should be adapted to different age groups and shared between the DPAs (PT). Tools could also be designed to evaluate what the students have learnt (FR).

4. The envisioned role of DPAs in the implementation of the Resolution

The DPAs surveyed envisioned taking different roles in the implementation of the resolution. For some, it should strive to promote and raise awareness around the Resolution, and more broadly the issue of data protection to expert groups (CH), relevant stakeholders (PT, BK) and the general public

(GI). For Mexico, it should also promote the updating of the Framework in order for it to stay relevant. The INAI also mentioned the necessity to disseminate indicators, to measure the effectiveness of the framework.

DPAs can also support the development and the sharing of educational resources in relation with relevant stakeholders (FI/LU) as well as other DPAs (JE). Albania also mentioned the necessity of developing online tools to enhance teacher training.

Most DPAs highlighted the role of the DPAs as part of, or as coordinator of a network, whether at the international level between DPAs (ME, JE) or at a national level with government agencies (MU, IT), but also other stakeholders (PH, BK, ME, LU).



## Annex 2



### Survey information - Summary report of *25 August 2020*

#### **Legal framework and practices of data protection authorities regarding the exercise of the rights of minors**

#### **Putting into perspective other international initiatives on the issue of minors' rights**

##### *Disclaimer*

*This summary report has been submitted to the data protection authorities mentioned for approval and modified accordingly for final publication of the current study. By proposing a collection of legal information that refers to legal frameworks that were the subject of a survey in 2018 updated in 2019, this overview is based on the responses of 46 Data Protection Authorities. This report does not claim to provide an exhaustive overview or an up-to-date inventory of the legislative environment that might have been subject to changes since then.*

##### ***The purpose of this report is twofold:***

###### *In part 1.*

*It aims to **draw up an inventory of the existing legal framework** in the various States with regard to the exercise of their rights by minors, and in particular their rights to data protection. To this end, it summarises **the responses of 46 data protection authorities** out of a hundred or so consulted during a survey carried out by the CNIL, coordinator of the International Digital Education Working Group (DEWG) in 2018 and 2019.*

###### *In part 2.*

*It presents **a monitoring on various international initiatives and strategic orientations that are currently being revised and may bring into light new perspectives on the issue of minors' rights.***

## **1 Legal framework and practices of the authorities relating to the exercise of children's rights**

The mapping of the legal framework relating to the exercise of children's rights is based on a **synthesis of the results of the survey conducted by the CNIL on behalf of the DEWG in 2018 and**

2019<sup>5</sup>, supplemented by focuses that shed light on the initiatives carried out by certain data protection authorities.

An overview of the responses of the national and regional authorities leads to the organisation of the responses according to whether the juvenile is recognised in principle capable (1.2) or incapable with regards to exercising his or her privacy rights on his or her own (1.1).

## 1.1 The inability of the minor to exercise his or her rights alone

### 1.1.1 The inability in principle

In **18 States or regions**, the juvenile is classically recognised as incapable of exercising his or her rights in general, and his or her computer rights and freedoms in particular. They must go through their legal representatives (parents, guardian) to assert them.

- ➔ Bulgaria, Burkina Faso, Canada, Greece, Colombia, Estonia, Bavaria (Germany), Kosovo, Lithuania, Republic of Mauritius, Mali, Mexico, Netherlands, Philippines, Slovenia, USA, Albania, Georgia.

### 1.1.2 Towards the recognition of a certain ability

In some countries, the inability of the minor to exercise his or her rights remains the general law, but there have been some developments.

In **Italy**, in 2017, the Italian Parliament passed a **law against cyber-bullying**, which allows a **minor of 14 years old or over to request for the removal** of the problematic content on his or her own. This must be done within 48 hours.

**Luxembourg** is a good example of the influence of European and international standards on the classic model denying minors the capacity to exercise their rights. For **data processing based on Article 8 of the GDPR** (legal basis for consent, direct offer of information society services), **the Luxembourg data protection authority (CNPD) has considered that children over 16 years** can exercise their data protection rights alone. This threshold corresponds to the choice made by Luxembourg as to the age at which a minor can consent alone to the processing of his or her data pursuant to Article 8. **The CNPD has therefore interpreted the text of the GDPR as establishing a logical link between the capacity to consent and the capacity to exercise one's rights. Moreover, for other data processing** (e.g. the right to object to a photo taken in a school setting), the Civil Code should apply in principle. It sets the age of legal majority at 18 years old. Below this threshold, only parents or the legal guardians may in principle exercise minor's rights. Nevertheless, the CNPD argues in its response for a more flexible position. **It recommends to make room for the capacity for discernment, under the influence of Article 16 of the UNCRC Convention (International Convention on the Rights of the Child) which affirms the child's right to privacy.** This provision could, according to the Convention, *"prevent the Supervisory authorities from limiting the rights of access, rectification, opposition and deletion to parents alone"*.

In **Quebec**, the Commission for Access to Information (CAI) indicated in its 2019 response that, in principle, only parents could exercise the child's rights. Nevertheless, it noticed that the legislation on the protection of personal information refers to the "data subject" without distinguishing whether

---

<sup>5</sup> Data protection authorities were invited to specify the legal framework applying to children in their respective countries, in order to identify their level of autonomy in exercising their own data protection rights.

he is major or minor, which opens up the possibility of accessing a request to exercise one's rights by a minor. The Commission therefore admits that *"if a request for access, rectification, opposition or deletion were submitted by a minor, it would be appropriate to consider whether, given his age and discernment, this is an act that he can undertake alone to satisfy his ordinary and customary needs"*. **Thus, if the law does not formally recognise a minor's capacity to exercise his or her rights, the CAI considers the silence of the law to be an invitation to recognise it in practice, depending on his or her age and degree of discernment.** The CAI is also in **favour of recognising a digital majority**: it considers 14 years to be the appropriate age, since it corresponds to the threshold at which a minor can consent to care alone and is deemed to be of full age for all acts relating to his or her employment, the exercise of his or her art or profession.

Most recently, on June 12, 2020, it has to be noted that the Government of Quebec introduced a *Bill 64 - An Act to modernize legislative provisions respecting the protection of personal information*. This bill provides amendments of the laws governing the protection of personal information in the public and private sectors, in particular, regarding the consent of minors aged 14 and over (see sections 9, 16, 96, 102 of the current draft bill).

#### **FOCUS: in France**

As it stands, the **French law is based on the principle of the incapacity of the minor**, who must be represented by the holders of parental authority for all acts of legal life, and in particular the exercise of his or her rights. There are, however, exceptions to this principle. Indeed, in the field of medical research, Article 58 of the amended Data Protection Act allows *«a minor aged fifteen years or over to "object to the holders of parental authority having access concerning his/her data collected for research, study or evaluation purposes. The minor then receives the information provided for in Articles 56 and 57 and exercises his or her rights of access, rectification and opposition alone."*<sup>6</sup> This reform has been widely supported by the CNIL.

The issue of the ability of minors to exercise their data protection rights is the major focus of the CNIL's ongoing reflection on the rights of minors in the digital environment initiated in 2019. In view of the changes resulting from the General Data Protection Regulation (GDPR), the aim of this reflection is to clarify the French Commission's doctrine on the subject with a view to adopting recommendations that will clarify the applicable legal framework and enable it to offer practical advice that corresponds to the needs expressed and the reality of practices while respecting legal obligations.

**An online consultation was carried out on its website**, from 21 April to 8 June 2020, engaging the main stakeholders concerned (experts, the industry, national education authorities, children's rights organisations, NGOs, parents, etc.) and accounted more than 700 responses and contributions.

**A survey** commissioned by the CNIL, in December 2019, among 1,000 parents and 500 children aged 7 to 17, aimed to better understand the differences in the perceptions that parents and children may have of digital practices and the reality of these practices.

Working progress does not allow for communication on the feedback before the end of 2020.

---

<sup>6</sup> Today, art. 70, paragraph 3 of the French Data Protection Law (LIL) provides: *"For these processing operations, a minor aged fifteen or over may object to the holders of parental authority having access to data concerning him/her data collected for research, study or evaluation purposes. The minor then receives the information and exercises his or her rights alone."*

## 1.2 The capacity of a minor to exercise his or her rights

**Two approaches** were predominantly adopted by the participants from the panel study.

One is **objective**, and consists of setting an age threshold above which the minor can exercise his or her rights (1.2.1). The second is **subjective**, and focuses on the juvenile's maturity, capacity for understanding and discernment in order to grant him or her the power to exercise his or her rights (1.2.2).

An exception to this is the reply from the **Hong Kong Authority**, which stated that, in the absence of express exclusion, the *Personal Data Ordinance* in principle allows minors to exercise the rights it guarantees, without any age or other criteria being mentioned.

It should also be pointed out that **granting** the minor the ability to exercise his/ her rights may be without prejudice to the power of representation of the holder of the parental authority.

### 1.2.1 Objective capacity: the age threshold

**8 States or regions determine an age threshold.** The responses from the authorities reveal that this recognition is mainly based on two grounds:

- Either the capacity of the minor to exercise his or her rights beyond a certain age is **expressly recognised by law**: this is the case in Norway, Scotland and Hungary.
- Or the recognition of this capacity is the result of an interpretation **by the authority**, which makes it a consequence of the autonomous age of consent of the minor in Article 8 of the GDPR: this is the case in Jersey, the Czech Republic, Spain and the Land of Brandenburg.

In addition, another dividing line can be drawn depending on the **degree of sophistication of the approach adopted**.

Some states only introduce a **threshold**: absence of capacity below, capacity above.

In **Scotland**, for example, a person aged 12 or over is presumed to be of sufficient age and maturity to be able to exercise the right of access, unless there is evidence to the contrary. It is even specified that a child under the age of 16 may exercise the rights granted to him/her by the GDPR and express consent to the processing of his/her personal data if he/she is able to have such understanding, unless the contrary is demonstrated. "The person is considered to have such capacity when he or she has a general understanding of what it means to exercise his or her rights or to provide such consent".

Other countries or regions have refined the age cut-off technique.

In **Hungary**, the rights of a minor under the age of 14 can only be exercised by his/her parent or legal guardian. Between the ages of 14 and 16, they must be exercised jointly by the child and his or her legal guardian. After the age of 16, the child alone can exercise his or her rights.

Moreover, in the **Land of Brandenburg**, the principle is a threshold age of 16, which corresponds to the age chosen by Germany within the margin of appreciation left pursuant to Article 8 of the GDPR. The Land of Brandenburg has adopted a law for schools which gives pupils aged 14 and over a right of access without the need for parental consent in school matters.

### 1.2.2 Subjective capacity: maturity, discernment, understanding

**15 states or regions have elected to apply a subjective approach:** Ontario (Canada), Australia (Victoria), Switzerland (with a specific response from the canton of Basel along the same lines), Berlin (Germany), Thuringia (Germany), Hessen (Germany), Gibraltar, Israel, Japan, New Zealand, Slovakia, Slovenia, Turkey, United Kingdom (except Scotland)<sup>7</sup>.

- Responses from the State of Israel, Australia, Switzerland (including Basel), several German states, Slovenia, Japan and Ontario indicate that this criterion is directly derived from their **legislative framework**.
- For **New Zealand**, the child's capacity results from the absence of an age limit included in the Privacy Act 1993. The national data protection authority interprets this silence as allowing it to accept complaints from minors, depending on their degree of discretion.

The other authorities do not specify the basis of their response.

**The approach in Slovenia** is interesting in that it combines objective and subjective conditions: A minor over 15 years who has the capacity to understand the meaning and consequences of his or her actions and has a certain degree of maturity can exercise some of his or her rights before reaching the age of majority. The cumulative nature of the criteria suggests that before the age of 15 children are not considered to have a sufficient degree of discernment.

**Germany**, according to its Fundamental Law (Grundgesetz), defines that the child is the bearer of all fundamental rights and thus of the right to **informational self-determination** from birth. **For the exercise of rights, the decisive factor is the children's capacity of discernment**, i.e. whether the persons concerned are in a position to examine the consequences of the use of their data and thus to issue a binding opinion. Accordingly, children and adults have the right to decide on the disclosure or processing of their personal data and in case of doubt, the capacity of discernment will be examined individually, on a case-by-case basis, as there is no general legal definition. In the field of education, the legislation of several regions, including Bavaria, Berlin and Brandenburg, sets the age of discretion at 14.

In **Belgium**, if the minor is defined by the Civil Code as a person of either sex who has not yet reached the age of 18, a gradation in the protection of the minor is generally admitted. This transition is based in particular on the criterion of the child's capacity for discernment. Although this criterion may vary according to the practical and legal context, it is often situated between 12 and 14 years old.

In the **United Kingdom (UK)**, reference should be made to an annex to the 'Guide to the GDPR' drafted by the Information Commissioner's Office (ICO), where the data protection authority has looked at the specific situation of children<sup>8</sup>. With regard to the ability of minors to exercise their data protection rights, it is recalled that in Scotland presumption of sufficient maturity at the age of 12 does not apply in the rest of the UK. In the UK, capacity is assessed on the basis of the **child's level of understanding**, with no indication of an approach that would be considered reasonable in the majority of cases. However, a number of clarifications are made:

---

<sup>7</sup> <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf>

<sup>8</sup> <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-rights-do-children-have/>

- The general idea is that a child **should not be considered capable** if it is clear that he or she is acting against his or her best interests.
- If the child has been deemed capable of consent, then it will generally be reasonable to consider that he or she is also capable of exercising data protection rights.  
Like the Luxembourg authority, the ICO reasons here *a fortiori* to establish a link between the recognition of a capacity to consent and the possibility of exercising one's rights.
- If a child is recognised as capable then, just like an adult, **he or she can authorise someone to act in his or her name and on his or her behalf**. This person can be a parent, another adult, a representative such as a child advocacy service, an association or a lawyer.

#### **FOCUS Age Appropriate Design Code<sup>9</sup> in the UK:**

The Information Commissioner's Office (ICO), UK, has developed and published an *Age Appropriate Design Code* for the design of online services that may be used by minors to protect the privacy of those under the age of 18, as required by the data protection law<sup>10</sup>. This Code comes into force on 2 September 2020 following its effective adoption by Parliament on 12 August 2020. It was preceded by a broad consultation and is the subject of a large communication campaign. A transition period of 12 months after its entry into force should allow the online services industry to comply with its provisions, so that violations of these new rules will only apply from the autumn of 2021. This Code must be taken into account by the ICO and the courts when dealing with cases involving the data of minors<sup>11</sup>.

This **Code is intended to advise organisations on good practice in the collection of data by online services accessible to minors, as well as in the design of such services**. It covers social networking and applications, connected toys, video game platforms, streaming services and educational websites. Among the 15 standards developed, the Code notably provides for the prohibition of exploiting cognitive bias to collect a greater volume of data, and the deactivation of default geolocation. It can be noted that the age of users will have to be established at an appropriate level of certainty in view of the risks involved in processing the child's data and provides for the completion of a DPIA to take account of the various age groups.

In this context, ICO states that it was developed in the light of the International Convention on the Rights of the Child (UNCRC), and in particular the CRC guiding principle of the best interests of the child. A focus on the latter standard is particularly relevant to the issue of the capacity of minors to exercise their rights. In this, ICO has looked beyond the determination of capacity to the **effectiveness of the exercise of their rights by minors**. In fact, it requires the provision of "*visible and accessible tools to help children exercise their rights and report problems they encounter*". In this sense, the guide specifies several elements:

- **The mere possibility offered to children to exercise their rights is insufficient**: fulfilling this obligation implies helping them to do so,
- These tools **must be clearly visible** (e.g. by means of an easily identifiable icon);
- They must be **appropriate for the age of the user**,

<sup>9</sup> Published on the [ICO](#) website

<sup>10</sup> In accordance with what was required by a provision of the Data Protection Act 2018 (DPA) which incorporated the GDPR into the UK legal system, see Section 123 (1): "*The Commissioner must prepare a code of practice which contains such guidance as the Commissioner considers appropriate on standards of age-appropriate design of relevant information society services which are likely to be accessed by children* "

<sup>11</sup> CCA, Section 127 (3) and (4)

- The aim is to promote the design of **tools specific to the rights they promote** (e.g. a "download all my data" button for access rights and portability; a "delete all my data" or "select data to be deleted" button for the right to erasure; a "stop using my data" button for the rights to oppose and limit processing; a "correct" button for the right to rectification),
- **Include mechanisms to monitor the progress of a request and to communicate with the data controller.**

In **Ireland**, the choice between these different approaches continues to be a matter of debate, and the Data Protection Commission (DPC) has opted for a consultation organised between January and April 2019 into two streams: the one aimed at engaging adult stakeholders and industry, and the other aimed at children and young people. This feedback should provide information and be used for their approach to **guidance for children and young people** to ultimately be created on this topic and encourage the development of **codes of good practice** at sectorial level by representatives of the professional branches concerned and by government authorities.

**FOCUS the two streams of public consultation by the DPC's on Children's Data Protection Rights (Data Protection Commission of Ireland) - the following is an excerpt -:**

**1. The adult and industry stakeholders (Stream 1):** consultation of public and private stakeholders in the form of an online questionnaire<sup>12</sup>

**A number of questions focused precisely on the capacity of minors to exercise their rights of access and erasure:** the existence of an age threshold, the existence of other determining factors, and the involvement of parents.

The existence of an age threshold

To the questions *"At what age should a child be able to exercise their right of access / right to erasure"*, the most popular answer was "at any age". Two remarks in this regard:

- The **consultation was biased in favour of the exercise of rights by minors** since the three options proposed were respectively: "at any age", "12-15 years", "16-18 years";
- **The responses were more favourable to the child's exercise of his or her right to erasure than to access.**

The authority concluded that these issues **were considered as two separate issues**, and not part of a broader issue of a right to exercise one's data protection rights.

The existence of other determining factors

The synthesis of the responses revealed that a majority was in favour of taking other factors into account:

- The cognitive development of the child (intellectual and emotional),
- The level of education,
- Participation in extra-curricular activities,
- The existence of a disciplinary record,
- The child's family situation,
- The vulnerability of the child (is he/she disabled? emancipated?).

<sup>12</sup> <https://www.dataprotection.ie/en/news-media/public-consultation/whose-rights-are-they-anyway>



## Involvement of parents and limits to their power of representation of the child

A majority of responses stressed that **there should be a limit to the possibility for the child's legal representative to exercise data protection rights**, on the understanding that it is the child who is the holder of these rights. While parents should be able to exercise the rights of their youngest children, adolescents should be given a degree of control, particularly in situations where they might disagree with their parents.

In this sense, the majority considered that **from the age of 16 onwards, the child should have the possibility but not the obligation to seek the support or advice of his or her parents** when he or she wishes to exercise his or her rights.

**2. Towards children and young people (Stream 2):** a consultation addressing children and young people directly in their classrooms in order to gather their views<sup>13</sup>.

The DPC has created and distributed a pack of lesson plan materials specifically designed to help teachers explain and discuss data protection issues with their students. The DPC received a total of 50 submissions from different schools and Youthreach centres across the country, equating to the views of approximately 1,200 students based on an average class size of 25 pupils. The contributions concerned 40% of pupils aged 10-12, 30% of pupils aged 12-14, 24% of pupils aged 7-10 and 9% of pupils aged 14-17.

**Some of the questions addressed to them are of direct relevance to the exercise of the rights of minors:**

**"What age do you think you should have to be before you can sign up for a social media account without your parents' permission?"**

Responses to this question revealed that the **younger the children are, the more they suggest that this age should be higher**. For example, 8-9 year olds feel that they should wait until they are 16, while 13-14 year olds feel that they are at the age when they should be able to register on their own. The older children get, the more they feel that this threshold should be set lower in relation to their age, i.e. at 14-15 for pupils aged 15-17.

**"What age do you think you should have to be before you can ask any company for a copy of your personal data, or before you can tell them to delete your personal data?"**

It is clear from the answers given that the **minors interviewed believe that they should be able to exercise their rights at a very young age**. Indeed, the **answer favoured by around 40% of the pupils** is that they should be able to make access or erasure request **"at any age"**. 21% believe that they should be able to make it at "13 or younger". *Conversely*, only 13.5% of young people think it is necessary to be 18 or older to make access or erasure request.

**"Do you think you should be in charge of your own personal data? Or should your parents have a say?"**

It is interesting to note that although most children believe that they should be able to exercise their right to an access or erasure at any age or at a very young age, a **significant percentage also seems**

---

<sup>13</sup> <https://www.dataprotection.ie/en/news-media/public-consultation/some-stuff-you-just-want-keep-private-preliminary-report-stream-ii>



to think that parents should have a say in the management of their personal data, especially when they are younger.

- **44% of the students** considered that parents should have a role to play until the child is **18 years**: 90% of them were between 7 and 15 years,
- **19%** believe that parents should be able to intervene until the **child is 16 years**,
- **30% of the children felt that parents had no role to play**: the majority of these pupils were aged between 15 and 17 years old.

In concluding this study conducted by the Irish Data Protection Commission, the highlights of the two parts of the survey therefore revealed:

- **A favourable trend towards the exercise of their rights by minors.** Parents, for their part, see their involvement reinforced for the youngest, but limited as their child grows older.

- Clear expectations from children with regard to online services, applications and platforms regarding their obligation to explain what they do with their personal data. They believe that these companies could interact with children about their personal data in a **simpler, more transparent, accessible and flexible<sup>14</sup> way**.

- Finally, with regard to the views expressed by children and young people about their rights and responsibilities online and by their parents, younger children in primary school classes are likely to believe that their parents know everything better than anyone else and they ask for more parental control and involvement. While older children are more likely to think they are ready to manage their online activities, including the processing of their personal data on their own.

### FOCUS Subjective Determination of Capacity: The *Ontario* Example

On January 1, 2020, Part X of the Child, Youth and Family Services Act (CYFSA)<sup>15</sup> came into force in Ontario, providing that *"as of that date, every person, including children and youth, would have the right under the law to access and request correction of their personal information held by a service provider within specified time limits. **The relevant threshold applicable to the exercise of the rights of children and youth is not the age, but the capacity.** These rights may also prevail over the decisions of parents or guardians in the event of a conflict.*

The interest of this legislation for this study may seem *a priori* limited because of its **scope of application** to child protection service providers (e.g. Child welfare service, foster care, etc.). Nevertheless, it has led the Office of the Information and Privacy Commissioner of Ontario (IPC) to develop a practical **guide<sup>16</sup>** related to the application of the law, **part of which seeks to define more precisely the notion of capacity of minors by proposing an analytical grid.**

The main lines of the survey offer an interesting analysis grid:

#### **1/The need for capacity**

The individual must be able to consent to the collection, use or disclosure of personal information.

<sup>14</sup> Cf. computer graphics of the detailed responses by age group.

<sup>15</sup> <http://www.children.gov.on.ca/htdocs/English/professionals/childwelfare/modern-legislation.aspx>

<sup>16</sup> <https://www.ipc.on.ca/part-x-cyfsa/>

In order to do so, he must be able to:

- (1) Understand the relevant information that is relevant to the decision to consent or not to consent;
- (2) Understand the reasonably foreseeable consequences of the decision to give, refuse or withdraw consent.

NOTES:

- **It is the responsibility of the service provider to assess the capacity**
- **Capacity is presumed** unless there are reasonable grounds to believe that the person is not capable (e.g., the infant).
- The capacity is **assessed *in concreto***

1) The law does not establish **a link between capacity and age**.

2) Capacity may be **partial**: some people may be able to consent to some parts of their personal information but not others. For example, a child may be able to consent to the transfer of a large part of his or her social records to another service provider, but unable to appreciate the consequences of disclosing or not disclosing a particularly sensitive part of them.

**2/ Determination of capacity**

The IPC sets out good practices for determining a person's capacity to consent:

- **Provide all relevant information**, including the purpose of the proposed collection, its use and possible disclosure,
- Consider **asking them to repeat** relevant information they have been given to help assess their level of understanding,
- Ensure that a language barrier, language impairment or cultural differences do not affect the assessment of the individual's ability.

**3/ The consequences of the finding of incapacity**

- **Obligation to inform the individual of the consequences of such a finding** if it is reasonable to do so in the circumstances.
- This finding **relates only to the individual's rights under Part X** and does not affect other issues.
- **Opportunity to challenge** a finding of incapacity before the Consent and Capacity Board (an independent body that conducts hearings in disputes over issues such as a person's ability to make decisions about medical care, or the appointment of a representative to make decisions with regards to specific care for a person who is incapable of making his or her own decisions).

**FOCUS: The revision of the Children's Online Privacy Protection Act (COPPA) in the USA**

In the United States, the COPPA Act (1998) requires companies for the processing of minors' data under the age of 13 to obtain **their parents' consent**<sup>17</sup>.

This legislation has already been revised in 2013 to reinforce the obligation of parental consent and take into account new uses, and in particular to include geolocation, as well as audio files, photos

---

<sup>17</sup> FTC (2018) Happy 20th birthday, COPPA <https://www.ftc.gov/news-events/blogs/business-blog/2018/10/happy-20th-birthday-coppa> / <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance#step4>

and video in the definition of personal data. **But it seems that a new revision is necessary**, in view of the criticisms addressed to it.

To this end, the FTC has launched a <sup>18</sup>**public consultation in 2019** on the rules for the protection of minors online, with a view to the possible revision of COPPA. The COPPA incorporates issues relating to its effectiveness and scope.

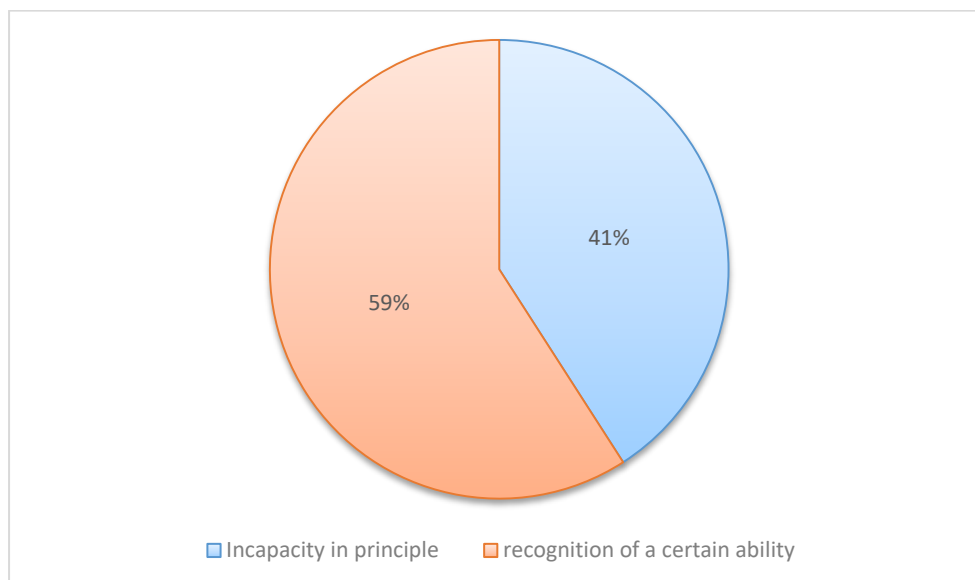
In the United States, leading children's advocacy, health and privacy groups<sup>19</sup>, as well as several Senators<sup>20</sup> pointed to excessive screen use and increased data collection in the wake of Covid-19 pandemic, and **have called on the FTC to investigate the children's digital media market** before proposing any changes to the COPPA Act's operating rules.

### 1.3 Elements of synthesis

The summary elements of this study, in its two parts (legal frameworks and the following monitoring of international initiatives), therefore reveal a favourable trend towards the exercise of their rights by minors. Parents, for their part, see their involvement reinforced for the youngest, but limited as their child grows older.

In summary of the elements presented above, it can be noted that the trends regarding the exercise of the rights of minors are as follows:

- The DPA responses show a **definite momentum in favour of the exercise of rights by minors**, and in particular their **data protection rights** : in total 18 countries or regions introduce an incapacity in principle, while 26 others have embarked on a path of some capacity.

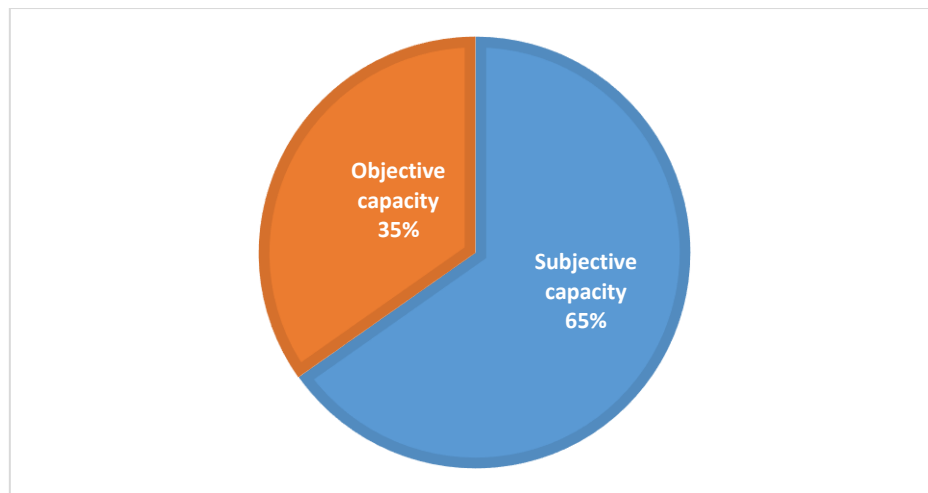


<sup>18</sup> FTC (2019), Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule <https://beta.regulations.gov/document/FTC-2019-0054-0001>:170,000 comments received, including 80,000 made public

<sup>19</sup> Center for Digital Democracy (2019) Leading child advocacy, health, and privacy groups call on FTC to Investigate Children's Digital Media Marketplace Before Proposing any Changes to Privacy Protections for Children

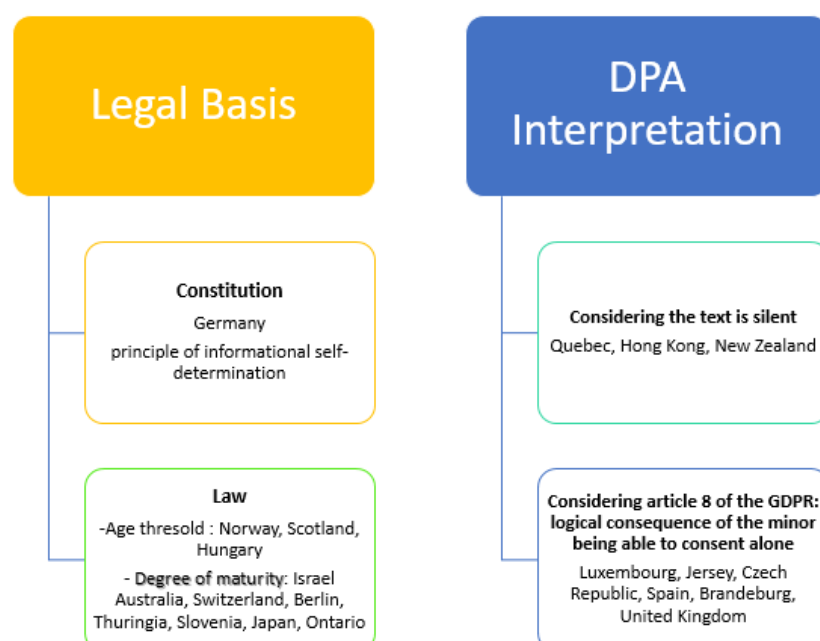
<sup>20</sup><https://www.democraticmedia.org/article/leading-child-advocacy-health-and-privacy-groups-call-ftc-investigate-childrens-digital-0>  
[file:///C:/Users/psr/Documents/Children%20Doc/COPPA/Action%20Consultation%20FTC/Markey%20letter%20Senate%20to%20FTC%206\(B\)%20on%20children's%20privacy.%208%20May%202020.pdf](file:///C:/Users/psr/Documents/Children%20Doc/COPPA/Action%20Consultation%20FTC/Markey%20letter%20Senate%20to%20FTC%206(B)%20on%20children's%20privacy.%208%20May%202020.pdf)

- Moreover, this trend is based in particular on an interpretation of the **letter of the data protection texts**, but also on the **International Convention on the Rights of the Child (UNCRC)**.
- It is the **subjective capacity, by virtue of the degree of maturity of the minor, which seems to be preferred by those countries or regions** which have decided to allow minors to exercise their rights: 15 countries or regions have opted for the degree of maturity, and only 8 for the age threshold<sup>21</sup>.



- Granting minors the ability to exercise their rights to information technology and freedom can have several bases, summarised in the following diagram:

## Basis for granting minor the capacity to exercise their rights



<sup>21</sup> As a reminder, only 46 DPA responded to the survey.

## 2 International initiatives relating to the exercise of children's rights

---

### 2.1 The Council of Europe's draft Guidelines on the Children's Data Protection in an Education setting, of 12 June 2020<sup>22</sup>

In 1981, the Council of Europe adopted Convention 108, the first binding international instrument in the field of data protection. It was reformed in 2018 to become **Convention 108+**. Within this legal framework, the Consultative Committee of this Convention has drawn up draft recommendations identifying the issues and remedies available in education systems concerning the protection of children's data.

These guidelines, which were on the agenda of the March, 2020 meeting of the Consultative Committee of Convention 108, were postponed due to the Covid-19 epidemic, and will be reviewed at the end of September 2020. They were the subject of a first open webinar presentation at the initiative of the Council of Europe in July 2020.

Two salient points can be highlighted (subject to further changes in this text):

Firstly, the principle guiding these guidelines is the best **interests of the child**. This notion must be at the heart of all actions relating to children in the digital environment. It is **understood in an evolving way**, in the sense that the development of children's capacities from birth to majority must be taken into account, which implies adapting policies to make minors' rights effective. Within this framework, the child's opinion must be given increasing importance according to his or her age and maturity, as specified.

Secondly, they **seem to be largely in favour of a recognition of the evolving capacities of the minor to exercise his or her rights**. A number of elements converge in this direction, in the current stage of the text currently under discussion.

The same principles are also underlying another Council of Europe instrument adopted in 2018: **Recommendation CM/Rec(2018)7<sup>23</sup> on Guidelines to respect, protect and fulfil the rights of the child in the digital environment**, which has become a key reference for the Organisation's continuous work on data protection, for all activities relating to the rights of the child in the digital environment, as well as for relevant action taken by national governments.

### 2.2 The European Network of Ombudspersons for Children (ENOC): Position Statement of 27 September 2019

The European Network of Ombudspersons for Children (ENOC) is an **organisation which brings together independent institutions responsible for the promotion and protection of children's rights** as formulated in the Convention on the Rights of the Child (CRC). Founded in 1997, the ENOC network currently has 42 members in 34 European States.

---

<sup>22</sup> A new version has been produced [12June2020 T-PD(2019)06BISrev3].

<sup>23</sup> <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>

Its Annual General Assembly adopted a **Position Statement on 27 September 2019** which seeks to make **effective children's rights guaranteed by the UNCRC in the digital environment**<sup>24</sup>. To this end, the idea of the possible acknowledgement for children to exercise their rights has a prominent place in the mechanism.

In this sense, it advocates **methods of information and the design of tools adapted to children**, enabling them to access their rights without discrimination.<sup>25</sup>

The importance attached to the possibility for children to exercise their rights is even more eloquently illustrated in **Recommendation No. 9 to ensure access to reporting, complaint and redress procedures**. In particular, it urges:

- *"Develop **quick and easy access procedures** and **child-friendly information** about these procedures to **enable children to report concerns** about harmful content or cases of harassment, violence and abuse, and to make **complaints to industry and governments**, including social networking and technology companies, Internet providers and regulators".*
- *"In particular, ensure that regulatory protection procedures are in place to receive and **respond to reports from children**, parents or guardians of children of concerns about sexual predation, abuse and exploitation in all media and platforms".*

### 2.3 OECD Initiative: Revision of the 2012 Recommendation on the Protection of Children Online

A revision of the 2012 OECD Recommendation on the Protection of Children Online<sup>26</sup> was initiated in 2018 and is expected to result in a new text by the end of 2020. While the 2012 Recommendation has so far focused particularly on the protection of children as Internet users, the current draft revision aims to strike a new balance in the light of technological advances exposing children to a typology of increased <sup>27</sup> risks.

The various analytical reports and country consultations aimed to identify policy developments, legislative changes applicable to child protection on the one hand, and on the other hand, the potential impact of developments related to technological contexts, the digital uses of children online, as well as threats and new risks emerging in this rapidly changing landscape.

Amendments currently being developed in the Recommendation should encourage, inter alia, the creation of a comprehensive policy framework for a safe digital environment respectful of children's rights.

---

<sup>24</sup> "We, members of the European Network of Ombudspersons for Children (ENOC), call on governments, the European Commission and the Council of Europe to take all necessary measures to **respect, protect and fulfil children's rights** so that children and young people can enjoy the benefits and opportunities of the digital environment.

<sup>25</sup> V. recommendation 4.b on access of all children to the digital environment without discrimination

<sup>26</sup> OECD (2012). The Protection of Children Online [https://www.oecd.org/sti/ieconomy/childrenonline\\_with\\_cover.pdf](https://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf)

<sup>27</sup> A multi-stakeholder expert group has been set up under the auspices of the OECD **Working Party on Data Governance and Privacy in the Digital Economy (DGP)** to guide the updating work and take into account the new risks and digital skills identified for future development.

## 2.4 ITU-COP Initiative: the new 2020 Guidelines on Child Protection Online

The newly revised **Guidelines on Child Online Protection (COP)** <sup>28</sup> for policy makers, industry, parents and educators, as well as children were published on 23 June 2020 by the International Telecommunication Union<sup>29</sup>.

The new guidelines have been completely rethought, rewritten and redesigned to take into account the major changes in the digital landscape in which children live, such as the Internet of Things, connected toys, online games, robotics, machine learning and artificial intelligence.

They provide a comprehensive set of recommendations **on how to contribute to a safe online environment that empowers children and young people.**

They have been designed in the form of four guides which target respectively:

- **Children:** the resources proposed (a storybook for the under-9s, an activity booklet for the 9-11s and a campaign on social networks for the 12-18s) should enable them to learn how to behave when facing online risks, and **give them both the means to exercise their rights online and to take the opportunities offered by the Internet.**
- **Parents and educators:** to help them create a healthy, safe and empowering online environment for young people by emphasizing the importance of open communication and ongoing dialogue with children.
- **Industry:** The guidelines highlight in particular that children's rights must be taken into account at all stages of policies and processes (processing of content, digital environment tailored for respective children's age groups, etc.).
- **Policy-makers:** The guidelines promote inclusive national strategies, multi-stakeholder approaches through open consultation and discussion with children.

ITU and its partners have worked to develop a flexible, adaptable and readily useable framework , based on international standards and common goals, in particular the Convention on the Rights of the Child and the UN Sustainable Development Goals.

## 2.5 Initiative of the UN work on the CRC Convention

### 2.5.1 The UN Committee on the Rights of the Child (UNCRC)

The UN Committee on the Rights of the Child decided in 2018 to develop General Comments on **rights of the child in the digital environment.**

To this end, the Office of the High Commissioner of the United Nations for Human Rights (via the Committee on the Rights of the Child) launched a call for contributions, addressed to all interested parties, which was closed on 15 May 2019<sup>30</sup>. At the same time, **broad consultations with children**

---

<sup>28</sup> Launch on 23 June 2020 <https://www.itu.int/fr/mediacentre/Pages/pr10-2020-Guidelines-Child-Online-Protection.aspx>

<sup>29</sup> The International Telecommunication Union (ITU- COP (Children Online Protection) is the United Nations specialised agency for information and communication technologies (ICTs).

<sup>30</sup> 136 contributions received from States, regional organizations, United Nations agencies, national human rights institutions and commissioners responsible for children, children's and adolescents' groups, civil society organizations, academics, the private sector and other entities and individuals.  
[https://www.ohchr.org/EN/HRBodies/CRC/Pages/Submissions\\_Concept\\_GC\\_Digital\\_Environment.aspx](https://www.ohchr.org/EN/HRBodies/CRC/Pages/Submissions_Concept_GC_Digital_Environment.aspx)



(700 children in 26 countries) were undertaken and will contribute to enrich the draft observation comment.

The General Comments aim to strengthen the implementation of good practices and to elaborate what measures are required by States in order to meet their obligations to promote and protect children's rights in and through the digital environment, and to ensure that other actors, including business enterprises, meet their responsibilities.

**A first version of the document has been published<sup>31</sup>**. At this stage, several elements can be retained from the draft text:

- **Four fundamental principles** protected by the CRC constitute the prism through which the respect of all other rights must be seen: the principle of non-discrimination (art.2), the best interests of the child (art.3§1), the right to life (art.6), the right to be heard (art.12),
- The **evolving capacities of children** must be at the heart of the development of public rules and policies relating to the implementation of children's rights in the digital environment (§20),
- **States should prohibit targeted advertising directed at minors, regardless of age (§42),**
- States must ensure that there **are appropriate and effective judicial and non-judicial remedies for violations of children's rights** that are prompt, available and accessible to **children and their legal representatives (§45),**
- The **control systems in place, including parental control, must be balanced against the rights of the child**, in particular their right to freedom of expression and privacy (§57),
- The State must **insist that parents insist on the importance of respecting the child's right to privacy, and on their practices likely to infringe it** : sharing of photos and information about the child on social networks, system of parental control (§77).

**This draft text is subject to a second phase of consultation (open until 15 November 2020).** Taking into account these latest contributions will lead the Committee to decide on the content of the final version of the General Comment.

#### 2.5.2 The Special Rapporteur to the United Nations on the right to privacy

The UN Special Rapporteur<sup>32</sup> on the right to privacy launched a call for contributions<sup>33</sup> in July 2020, which will examine in his next annual report under the thematic action stream 'A Better Understanding of Privacy', **the specific theme of children's rights to privacy and data protection** (under the age of 18) and how this right interacts with the interests of other actors (business, governments, parents/guardians and others) and affects the evolving capacity of the child and the growth of autonomy, and what factors enhance or constrain this development.

Given the international scope of this field of investigation, an important part of the work is to understand the different points of view from around the world, and a particular interest will be given to the work, reflection and experiences of data protection authorities in relation to these issues.

---

<sup>31</sup>OHCHR (2020), Draft General Comment No. 25 (202x) : Children's rights in relation to the digital environment [https://tbinternet.ohchr.org/Treaties/CRC/Shared%20Documents/1\\_Global/CRC\\_C\\_GC\\_25\\_9235\\_E.pdf](https://tbinternet.ohchr.org/Treaties/CRC/Shared%20Documents/1_Global/CRC_C_GC_25_9235_E.pdf)

<sup>32</sup> Prof. Joseph CANNATA CI

<sup>33</sup> [https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/CFI\\_Privacy\\_and\\_Children.aspx](https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/CFI_Privacy_and_Children.aspx) Submissions must be received **by 30 September 2020**.



## 2.6 UNICEF initiative

In 2018, UNICEF published a <sup>34</sup>**guide on children's online privacy and freedom of expression**: companies can also find **practical advice to encourage them** to comply with the legal framework for the protection of personal data in order to respect children's rights in the digital world. It invites to:

- **Provide children with continuous access to** sites, products, services and applications with **age-appropriate content**;
- **Encourage and value children's productions** as responsible and committed citizens in society;
- **Give children more control** over how their profiles, images and personal information can be searched, accessed and deleted;
- Make the **conditions of use** simpler, concise, visible, clear, accessible and appropriate for children as they grow up;
- **Ensure that privacy settings are visible and compatible** with the target children, and provide better protection for children's accounts;
- **Limit opportunities to sell, share or monetize children's data** and restrict the use of children's data for marketing or advertising purposes.

## 2.7 European Union initiatives

- **The European Commission** launched on 15 June 2020 a **call for tender**<sup>35</sup> a **pilot project for an interoperable technical infrastructure dedicated to the implementation of child protection mechanisms such as age verification and parental consent**.

Ultimately, the aim is to identify the best approaches to carry out reliable age verification checks to prevent children from accessing inappropriate content, to reliably obtain parental consent, and to set up a cross-border age verification mechanism.

- **The EDPS (European Data Protection Committee)** has included the **development of guidelines on the protection of children's data** in its work programme for 2019-2020<sup>36</sup>.

---

<sup>34</sup> UNICEF (2018), Industry Toolkit : Children's online privacy and freedom of expression

[https://www.unicef.org/csr/files/UNICEF\\_Childrens\\_Online\\_Privacy\\_and\\_Freedom\\_of\\_Expression\(1\).pdf](https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf)

<sup>35</sup> [https://ec.europa.eu/research/participants/data/ref/other\\_eu\\_prog/other/pppa/wp-call/pp-call-document-pppa-agever-01-2020\\_en.pdf](https://ec.europa.eu/research/participants/data/ref/other_eu_prog/other/pppa/wp-call/pp-call-document-pppa-agever-01-2020_en.pdf)

<sup>36</sup> EDPS (2019) Work Program [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb\\_work\\_program\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf)

## Annex 3

# Report of the International Working Group on Digital Education

August 2020



---

2020 Conference of the Global Privacy Assembly

---

**Name of Office: The Office of the Privacy Commissioner of Canada**  
**Results of the Questionnaire regarding Implementation of the Resolution on e-learning platforms**

## INTRODUCTION

The e-learning Resolution, adopted at the 40<sup>th</sup> International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Brussels on October 2018, called upon all relevant parties in the field of e-learning to fully respect students', parents' and educators' ("individuals") rights to: i) protect their personal data and privacy; and ii) guarantee that the data collected is solely used for educational purposes in compliance with data protection law.<sup>37</sup> The Resolution was meant to assist educational authorities, e-learning platform providers, and manufacturers in meeting their data protection and privacy obligations towards delivering adequate and high-level guarantees to accompany the collection, processing, retention and disclosure of individuals' data in the educational environment. The Resolution also included a guide to assist ICDPPC members with the implementation of this Resolution.

The International Working Group on Digital Education (DEWG) presented their 2018-2019 Activity report at the 41<sup>st</sup> ICDPPC in Tirana among which the Office of the Privacy Commissioner of Canada (OPC Canada) produced a first *Report regarding the Implementation of the Resolution on E-Learning Platforms*.<sup>38</sup> It highlighted initial progress by data protection authorities on their engagement with government and school authorities, development of useful resources, and outreach activities. The report reiterated several of the recommended actions contained in the E-Learning Resolution's Implementation Guide for DPA's, and suggested follow up activities in 2019-2020.

As part of the DEWG's ongoing monitoring activities, a questionnaire pertaining to Action Item 3 surrounding the implementation of the Resolution on e-Learning Platforms was distributed to Working Group members **in February 2020**. Acknowledging that the implementation of such a comprehensive Resolution requires sustained efforts in the long term, the DEWG Secretariat asked members of the Working Group to complete a similar questionnaire as previously conducted in 2019 to inform a

---

<sup>37</sup> Resolution on E-Learning Platforms: <https://icdppc.org/wp-content/uploads/2019/03/dewg-Resolution-adopted-20180918.pdf>

<sup>38</sup> The report produced in English and in French can be made available on request to Melissa at the OPC and Pascale at the DEWG Secretariat

comprehensive overview of global progress regarding initiatives related to the promotion of the Resolution and identification of ongoing Codes of Practice in this area.

## **SUMMARY OF SURVEY RESULTS**

In February of 2020, staff of the Commission nationale de l'Informatique et des Libertés (CNIL) and the Office of the Privacy Commissioner of Canada (OPC) distributed a questionnaire to all DEWG members to collect information about the implementation of the 2018 Resolution on e-learning platforms.

We received responses from 11 authorities.<sup>39</sup> A summary of these responses can be found below.

### **Media coverage and dissemination of the Resolution**

The survey results generally demonstrate that while authorities are adopting different dissemination approaches, media coverage is low.

Several authorities engaged in virtual presentations to disseminate information about the Resolution and the work of the DEWG. France noted that the CNIL was invited as an expert panelist at one of UNESCO's weekly webinars about "the educational dimensions of the COVID-19 and Protecting learners data, privacy and security in the global shift to online learning," with an audience of 300 participants. They also noted that there may be some follow-up action at the UNESCO level aimed at aligning recommendations and supporting the creation of frameworks based on multi-stakeholder cooperation between public, private and civil sectors, regulatory authorities and education institutions.

Likewise, the CNIL of France was invited as an expert panelist at the Council of Europe Webinar addressing the following questions: "What does the right to data protection imply in an educational setting? What schools have to do, and what should they stop doing?" The CNIL included comments that this Webinar served two purposes. Firstly, to provide an overview of the work DPAs have done in relation to the 2016 and 2018 Resolutions; secondly, to make suggestions for the draft Guidelines of the Council of Europe on children's data protection in an educational setting. To note, CNIL indicated that DPAs may have a chance to respond to the formal call for comments on the draft Guidelines with the aim of improving or enhancing certain aspects as soon as published by the Council of Europe.

Other authorities, such as Burkina Faso, Italy and Switzerland indicated that they have published the Resolution on their website. For instance Italy specified that they have a special section of their website dedicated to privacy and school, in which the Resolution is featured.

Additionally, some authorities undertook additional initiatives to increase dissemination. Mauritius engaged in a full day workshop with press in attendance in January 2020. During this workshop, the training toolkit was presented to an audience of approximately 500 actors from different sectors of the economy. The Italian DPA noted that it contributed to spreading awareness of the Resolution through its standard channels of dissemination. Burkina Faso indicated that there have been initiatives to this effect at a national level, specifying that suppliers and designers declare their platforms to the CIL and work to integrate into their terms and conditions the principles of their April 20, 2004 Law 010-2004 / AN on the protection of personal data. To this end, CIL advises suppliers and designers on online platform design projects for the protection of personal data and ensures that the purposes of data collection, use and communication are adapted to the educational context in order to avoid any risk of inappropriate, unauthorized or illegal data processing. Finally, Gibraltar noted that they will provide guidance to education departments and schools.

---

<sup>39</sup> Burkina Faso, Cyprus, France, Gibraltar, Italy, Mauritius, Mexico, Philippines, Poland, Portugal, Switzerland.

**Recommended action Item:**

The Resolution's implementation guide for DPAs encouraged members to post the Resolution on their websites and other publications, share through communications and outreach channels, such as social media, and cite it in their work related to children and youth, and to education.

**Contact with relevant government or education authorities and Feedback from school authorities and other educational partners**

The Philippines noted that their National Privacy Commission (NPC) has been coordinating with CHED, the Department of Education, and other educational institutions, regarding the integration of Data Privacy in school curriculum. They have also engaged with educational institutions to help them launch their 2020 Kabataang Digital (Digital Youth) program, which specifically targets the online protection of children's data privacy. Their goal with the Kabataang Digital program is to reach even remote communities through their ground work. To accomplish this goal and facilitate the program launch, the NPC has connected with telecommunication companies and international NGOs focusing on children, and educational institutions.

Burkina Faso reported having a series of exchanges between the Ministry in charge of education and the CIL. The creation of a working group aimed at supporting digital education for students and teachers in the primary and secondly levels derived from these exchanges. This working group is still active and is working to integrate digital education into the curricula.

Switzerland noted that they actively participate in the "Jeunesse et medias" experts' group, which is managed by OFAS (l'Office fédéral des assurances sociales/ "the Federal Social Insurance Office").

Italy reported that contact with education authorities on e-learning has been increasing due to the exponentially higher use of e-platforms resulting from the Covid-19-caused closure of schools.

Cyprus also confirmed that they have had contact with relevant government or educational authorities. Mauritius reported that the Ministry of Education is responsible for all communication to schools in Mauritius.

France is further coordinating actions to disseminate new recommendations for good practice in schools for implementing compliance with GDPR obligations.

**Recommended action Item:**

The Resolution's implementation guide for DPAs encouraged members to share the Resolution with government, educational authorities, policy-makers, and other relevant stakeholders in order to stimulate conversations on the important issues this Resolution addresses and influence related policies and laws.

The current period of online educational continuity poses technology and privacy-related challenges, and has consequently reinvigorated the urgent need to create trust with digital tools in educational settings and a fair playing field for everyone when connecting to such eLearning platforms.

Where DPAs have reached out to these entities, the Working Group asks that you continue to track interactions for the purposes of future reporting to the DEWG on dissemination of the Resolution.

DPAs are encouraged to communicate with the abovementioned stakeholders, where DPAs have not yet engaged.

### **Feedback from the industry sector such as e-learning platform providers and manufacturers**

Survey responses reveal that feedback from the industry sector is limited, with two of the authorities reporting having received feedback from the industry sector (Mauritius, Burkina Faso).

Mauritius reported that the Ministry of Education has a long-standing collaboration with Microsoft, which they were able to leverage into procuring funding from Microsoft for a local firm to facilitate the adoption of Office 365 and Microsoft Teams platform. Credentials were set up for 8,500 teachers and about 56,000 students from Grades 10-13 on Microsoft Teams. The Ministry of Education encouraged students and educators to use some specific video-conferencing platforms during Covid-19 confinement, and the Data Protection Office prepared soft copies of materials for the Open University to teach Data Protection.

Burkina Faso noted that suppliers and designers have been able to integrate the protection of personal data and the resolution on privacy by design into the platform development processes due to the various awareness-raising activities the CIL Burkina Faso engaged in. They also report an increasing number of platform declarations<sup>40</sup> from these actors.

The Philippines noted that they are open to having further discussion in this area and in raising data privacy awareness for school children.

Cyprus and Switzerland both reported that they have not received industry feedback.

#### **Recommended action Item :**

DPAs are encouraged to share the Resolution with industry stakeholders such as e-learning platform providers and manufacturers in their interactions with these organizations.

The Working Group asks that you continue to track interactions for the purposes of future reporting to the DEWG on dissemination of the Resolution and more globally of eLearning platforms used in a privacy protective manner at school

### **Any progress in implementing the Resolution domestically or in planning its implementation in 2020?**

Nearly all respondents reported having made some progress in implementing the Resolution domestically or in planning its implementation in 2020 (Burkina Faso, Cyprus, Italy, Mauritius, Philippines). Italy indicated that their DPA has carried out activities to inform and raise awareness on

---

<sup>40</sup> CIL Burkina Faso receives platform declarations from private sector developers when they have a new platform they are testing

the privacy risks and responsibilities of using e-learning platforms as indicated in the Resolution, upon which they elaborate in question E. Cyprus reported being in the process of consultations with the Ministry of Education on remote/distance education during the pandemic, and noted that these have taken into account the Resolution.

In 2019, The Philippines NPC had a soft launch of the Kabataang Digital (Digital Youth) program as part of the PSST! Communication Campaign held at the University of the Southern Philippines, Cebu.

Burkina Faso reported that the CIL intends to encourage the Ministry in charge of national education to implement the Resolution. They have also included plans to verify and enforce compliance with platform design regulations in their 2020 activity plan.

Mauritius reported having engaged in a set of different activities to implement the Resolution domestically. Their Data Protection Office (DPO) organized five sessions of online trainings and webinars for educators and school rectors, including a free training from Dale Carnegie on 'How to engage your students online.' They also recruited a local firm to make videos aimed at students and training educators, and Ministry of Education IT staff created videos at the Open University of Mauritius, which were aired on educational television channels. Further, the Mauritius DPO published guides on their website and established teams of two champions within each secondary school, who received in-depth training for the purpose of helping other educators and students from their respective schools. Finally, Mauritius noted that their DPO also provides advice to the Ministry of Education and other organizations on matters including online learning.

France reported that a comprehensive national event (called "Etats Généraux") or a French Convention<sup>41</sup> on Digital Education will take place on 4 and 5 November 2020, where the Ministry of Education will gather all stakeholders concerned nationally around this event, namely teachers, principal and Heads of schools, inspection bodies, academies, local authorities, parents, middle school and high school students, non-formal education associations, ed tech industry for education, etc. During that event, progress on a Code of Conduct between the Ministry and the Ed tech sector oriented towards education could also be discussed (to be confirmed within the further agenda)<sup>42</sup>.

The objective of that event is twofold: to learn all lessons from the use of digital technology during the lockdown period, i.e. both good practices and difficulties encountered by teachers [educators, school administrators, and families] will be the major focus of interest built upon sharing of their feedback experience, and to have the Ministry continue to strengthen a concerted digital strategy for education. Comments are being published regularly on [the dedicated platform](#)<sup>43</sup>, in order to feed the public consultation until 4 and 5 November 2020.

### **Development of any Guidelines or emerging codes of conduct**

Survey results demonstrate that several authorities are developing and adopting guidelines and that codes of conduct are emerging in relation to the Resolution.

The Philippines NPC is coordinating with different sectors and industries in developing codes of conduct. Particular guidelines specific to the needs of the sectors and industries are likewise being developed from the feedback and recommendations of the industries themselves to determine the issues to be prioritized.

In April, 2020 Mauritius' DPO published a guide on data protection for health data and artificial solutions in the context of the Covid-19 pandemic.

---

<sup>41</sup> Articulated around one key topic: "Thinking digital for education in a transforming educational space-time"

<sup>42</sup> <https://etats-generaux-du-numerique.education.gouv.fr/pages/cp-20200626>

<sup>43</sup> [the dedicated platform](#) <https://etats-generaux-du-numerique.education.gouv.fr/>

Burkina Faso noted that CIL is working on establishing a practical guide over the course of 2020.

The Cyprus DPA indicated that they ordered the Ministry of Education to proceed and / or refrain from actions or omissions in order to meet the requirements set out in GDPR Regulation. The Cyprus DPA is also currently reviewing results of a compliance audit questionnaire, which addresses the exams and assessments that students wrote and performed remotely during the pandemic confinement.

The National Data Protection Commission of Portugal defined a set of guidelines for different actors involved in the processing of personal data, with the goal of insuring compliance with data protection legislation and to minimize the privacy impact of distance learning technologies.

The Italian Supervisory Authority (SA) adopted guidance on distance learning and data protection on March 26, 2020 in response to the increase in e-learning due to the Covid-19 context. Accompanying this guidance, the SA raised awareness of the need to manage e-learning platforms in full compliance with the data protection principles by writing a letter from the Chair of the SA to the Ministries of Education, of University and Research, and of Equal Opportunities and Family.

France reported that since 2019 there has been a project underway to establish a code of conduct. This project is being run by a national professional organization, mentioned in the CNIL's 2019 questionnaire response that supplies the National Education sector with platforms and digital resources. In 2020, the CNIL further collaborated with this organization in the counselling process towards finalization of the code to ensure that it would meet CNIL requirements when completed. At the end of this process, the code will need to be approved by all parties concerned.

Poland responded that taking the current Covid-19 context, in which education is taking place solely in an online environment with remote learning methods, the Personal Data Protection Office (UODO) has issued a Guide for schools. The Guide addresses good practices for keeping data secure during online lessons and includes twenty principles for teachers, students, and those in charge of schools to keep in mind. UODO has published this guide on their website and noted that with the help of the Ministry of National Education, it will reach all schools and educational institutions.

UODO received a letter from the authors of the code of conduct for education, stating that they had added a new chapter into the draft code, in which regulations for conducting remote teaching, including e-learning training, are described<sup>44</sup>. UODO also noted that this draft has not yet been submitted to their President for approval; it is currently with developers as they establish their plan for consulting with controllers and other entities potentially interested in its future uses.

Switzerland mentioned there hasn't been any guidelines developed or emerging codes of conduct.

#### **Recommended action Item :**

The Resolution's implementation guide for DPAs encouraged authorities to use the Resolution as a starting point to develop guidelines related to e-learning platforms and their data processing practices.

The Resolution's implementation guide for DPAs states that, where possible, DPAs should work with all relevant stakeholders to develop Codes of Practice governing the use of e-learning platforms. Codes of Practice may be a good avenue for addressing matters related to the drafting of contracts of services by e-learning platform providers, setting minimum standards on what is to be found in said contracts.

---

<sup>44</sup> The project is available in Polish at <http://rodo-w-oswiacie.pl/kodeks-postepowania-calosc/>

Where guidelines or Codes of Practice are being developed or in existence, the documents should be shared amongst Working Group members to encourage a dialogue regarding experiences, and to leverage resources. In line with this, DPAs are invited to have their related guidelines or Codes uploaded on the CIRCABC platform to be shared in the relevant classification.

### **Adaptation of resources and informational sessions to raise awareness on the data protection risks and mitigation measures identified in this Resolution**

Survey responses suggest that authorities are adapting a variety of resources and informational sessions to raise awareness of the data protection risks and mitigation measures identified in this Resolution.

The Philippines reported that the Kabataang Digital program will include the development of written resources to help children understand the basics of data privacy and protection. The Philippines NPC is also going to create videos for kids and mobile applications to facilitate children protecting themselves online.

Mauritius reported that advice is freely given to organizations and students involved in online and e-learning platforms.

Burkina Faso noted that in 2014 the CIL initiated a national campaign on digital education and the general risks associated with the usage of Information and Communication Technologies (ICTs) and the protection of personal data. This campaign is ongoing.

Italy noted that their SA recently collaborated with the Ministry of Education to elaborate some frequently asked questions (FAQ) on distance learning, with particular focus on the legal basis and transparency obligations set forth by data protection legislation.

France reported that the CNIL provided multiple GDPR training sessions in 2019-2020 as part of their continuous national training plan for heads of establishments and education executives within the IH2EF (the Institute of Higher Studies in Education and Training). In order to promote the protection of personal data, particularly that of students, the CNIL also published a series of practical resources<sup>45</sup> on their website during the Covid-19 health crisis, for teachers, school leaders and parents to draw upon when choosing which e-learning tools to use.

France also noted that the French Ministry of Education's guidebook "continuité pédagogique" (March 20, 2020 version)<sup>46</sup> is addressed to teachers, students and families. It indicated that in order to make

<sup>45</sup> Outils de la continuité pédagogique : les conseils de la CNIL. Published April 8, 2020. Available :

<https://www.educnum.fr/outils-de-la-continuite-pedagogique-les-conseils-de-la-cnil>

COVID-19 : les conseils de la CNIL pour utiliser les outils de visioconférence. Published April 9, 2020. Available :

<https://www.cnil.fr/fr/covid-19-les-conseils-de-la-cnil-pour-utiliser-les-outils-de-visioconference>

Coronavirus - COVID-19 : informations et recommandations pour les établissements scolaires, les personnels et les familles. Available : <https://www.education.gouv.fr/coronavirus-covid-19-informations-et-recommandations-pour-les-etablissements-scolaires-les-274253>

COVID-19 – Continuité pédagogique Protocole à destination des professeurs du 1er degré devant assurer une continuité pédagogique. Available : <https://www.education.gouv.fr/sites/default/files/2020-03/continuit-p-dagogique---protocole-destination-des-professeurs-1er-degr--52029.pdf>

COVID-19 – Continuité pédagogique Protocole à destination des professeurs du 2nd degré devant assurer une continuité pédagogique : <https://www.education.gouv.fr/sites/default/files/2020-03/continuit-p-dagogique---protocole-destination-des-professeurs-2nd-degr--52032.pdf>

<sup>46</sup> Coronavirus – COVID-19 Vademecum continuité pédagogique March 20, 2020 version available :

<https://www.education.gouv.fr/sites/default/files/2020-03/coronavirus-covid-19-vademecum-continuit-p-dagogique-66201.pdf>



educational sessions immediately available online, school districts were instructed to rely on the CNED (a free and privacy-compliant distance learning organization that collaborates with the French Ministry of Education), which has created the online platform “Ma classe à la maison” (My class at home).

**Recommended action Item :**

The Resolution’s implementation guide for DPAs invited members to post the Resolution on their websites and other publications, share through communications and outreach channels, such as social media, and cite it in their work related to children and youth, and to education.

As part of this effort, the Resolution suggests that DPAs prepare educational resources (or leverage those prepared by others) and, where possible, act as a resource to offer information and share best practices. Efforts can include organizing information sessions to raise awareness on the data protection risks and mitigation measures identified in this Resolution.

Where promotional and awareness materials exist, the materials should be shared amongst Working Group members to encourage a dialogue regarding experiences, and to leverage resources.

**Other noteworthy initiatives**

Italy reported that its DPA takes part in a working group coordinated by the Ministry of University and Research, which is undertaking a project addressed to young people, schools, teachers, and parents, called “Connected Generations.”

Mexico reported that as part of their annual Data Protection Day celebrations, their DPA approached school authorities from various elementary schools to hold conferences and awareness workshops on personal data protection. These workshops were intended to inform teachers and students about the main risks related to privacy, and to share personal information-protection recommendations with them. The INAI Mexico also published a series of tweets<sup>47</sup> on the subject.

The INAI Mexico also developed online materials for children, adolescents and data controllers. These resources include:

- Translated materials from the Office of the Privacy Commissioner of Canada,<sup>48</sup> which include advice on the protection of personal data when surfing the Internet and using mobile devices, social networks, and more.
- Recommendations to keep privacy and personal data safe in the digital environment.<sup>49</sup>

---

<sup>47</sup> INAI Tweets Available : <https://twitter.com/INAIMexico/status/954046335082291200?s=20>

<https://twitter.com/Igparranoriega/status/954027848070778881?s=20>

<https://twitter.com/INAIMexico/status/954043840175988736?s=20>

<https://twitter.com/INAIMexico/status/958521487908114432?s=20>

<https://twitter.com/INAIMexico/status/953612986844958720?s=20>

<https://twitter.com/JosefinaRomanV/status/1225611700625383425?s=20>

<https://twitter.com/INAIMexico/status/1225463597968560129?s=20>

<https://twitter.com/INAIMexico/status/1172275271451516928?s=20>

<https://twitter.com/INAIMexico/status/1142434322235789313?s=20>

<https://twitter.com/INAIMexico/status/1004090610570219520?s=20>

<sup>48</sup> [http://inicio.ifai.org.mx/Guias/Material\\_Primeria\\_4o\\_6o.pptx](http://inicio.ifai.org.mx/Guias/Material_Primeria_4o_6o.pptx)

[http://inicio.ifai.org.mx/Guias/Material\\_Secundaria.pptx](http://inicio.ifai.org.mx/Guias/Material_Secundaria.pptx)

[http://inicio.ifai.org.mx/Guias/Material\\_Preparatoria.pptx](http://inicio.ifai.org.mx/Guias/Material_Preparatoria.pptx)

<sup>49</sup> Recomendaciones para mantener segura tu privacidad y datos personales en el entorno digital. Available :

[http://inicio.ifai.org.mx/GuiasTitulares/5RecomendacionesPDP\\_Web.pdf](http://inicio.ifai.org.mx/GuiasTitulares/5RecomendacionesPDP_Web.pdf)

- An interactive questionnaire derived from the recommendations to keep privacy and personal data safe in the digital environment.<sup>50</sup>
- A Privacy Settings Guide for Major Social Networks, which provides users with instructions to properly configure their privacy and security settings on social media accounts.<sup>51</sup>
- A parental supervision tool guide, which gives parents information on different supervision tools available.<sup>52</sup>

## **Recommendation**

It is recommended that DPA activities continue to be tracked to monitor success and impact in advancing and disseminating the Resolution. Further monitoring would enable data protection authorities, and information and privacy commissioner offices to incorporate the follow up recommendations, found within the document, into their outreach and engagement planning. Ongoing reporting in this area could be used to develop best practices, lessons learned, and contribute to an understanding of why some initiatives may not have been adopted with a view to helping plan future activities.

---

<sup>50</sup> Test : ¿Cómo te proteges en el entorno digital ? Available :

<https://docs.google.com/forms/d/e/1FAIpQLSe39JYTKAMTSLgmOLrEvwVsuE9zZFeMZZAjosYF09AJIT00A/viewform>

<sup>51</sup> Guías para Titulares. Available : <http://inicio.ifai.org.mx/SitePages/guias-para-titulares.aspx>

<sup>52</sup> Herramientas o aplicaciones de Supervisión Parental en Internet. Available :

<http://inicio.ifai.org.mx/Guias/GuiaSupervisionParental.pdf>

## Annex 4

CIRCABC – Folder tree - Revised 15 April 2020

---

### **A. LEGAL INSTRUMENTS AND RESOLUTIONS ON PRIVACY EDUCATION AND DIGITAL RIGHTS**

- a. International legal instruments on privacy education and digital rights
- b. National legal instruments on privacy education and digital rights
- c. Resolutions / Declarations on privacy education and digital rights

### **B. SURVEYS– PUBLICATIONS ON DIGITAL EDUCATION, TRAINING, AI IN EDUCATION**

- a. General studies– Reports on digital education, training, AI in education
- b. Specific studies– Publications by DPAs, and the DEWG related to digital education, training, AI in education

### **C. AWARENESS-RAISING ON THE EXERCISE OF DIGITAL RIGHTS**

- a. Educational resources on children's rights
- b. Procedure for requesting access, information intended for children
- c. Complaints mechanisms for minors
- d. Consultations – surveys / study reports

### **D. EDUCATIONAL RESOURCES FOR STUDENTS**

- a. Resources / videos clips/ movies/ games/ comics/ practical tutorials
- b. Posters/ flyers

### **E. STOCKTAKING ON NATIONAL COMPETITIONS**

- a. Inventory of DPAs' competitions
- b. Guide for Data Protection Competitions

### **F. EDUCATIONAL RESOURCES FOR PARENTS**

- a. Guides
- b. Information Notices / exercising of rights

### **G. TEACHING RESOURCES**

- a. Competency Frameworks
- b. Lesson plans and Discussion Guides
- c. Manuals / teaching handbooks
- d. Mixed ready-to-use educational kits (teachers/ students)

### **H. TRAINERS' MATERIALS**

- a. Questionnaire to evaluate the level of trainers
- b. Trainers' packs

### **I. E-LEARNING PLATFORMS AND REMOTE LEARNING**

- a. Pedagogical eLearning platforms
- b. Study reports/ Surveys
- c. Guidelines / Codes of Practice
- d. Tutorials, posters, flyers