Survey information - Summary report of *15 September 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**[1], 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

[1] 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.

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 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****."* [2] 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.

[2] 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.*** *»*

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.

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)[3].

- 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-

[3] https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf

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[4]. 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:

- 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* [5] **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[6]. 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[7].

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

[4] 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/

[5] Published on the ICO website

[6] 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 "*

[7] CCA, Section 127 (3) and (4)

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**,
- 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[8]

[8] https://www.dataprotection.ie/en/news-media/public-consultation/whose-rights-are-they-anyway

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?).

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[9].

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

[9] https://www.dataprotection.ie/en/news-media/public-consultation/some-stuff-you-just-want-keep-private-preliminary-report-stream-ii

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 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**[10] **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

[10] Cf. computer graphics of the detailed responses by age group.

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)[11] 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**[12] 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.

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

[11] http://www.children.gov.on.ca/htdocs/English/professionals/childwelfare/modern-legislation.aspx
[12] https://www.ipc.on.ca/part-x-cyfsa/

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[13].**

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 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 [14]**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.

[13] 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

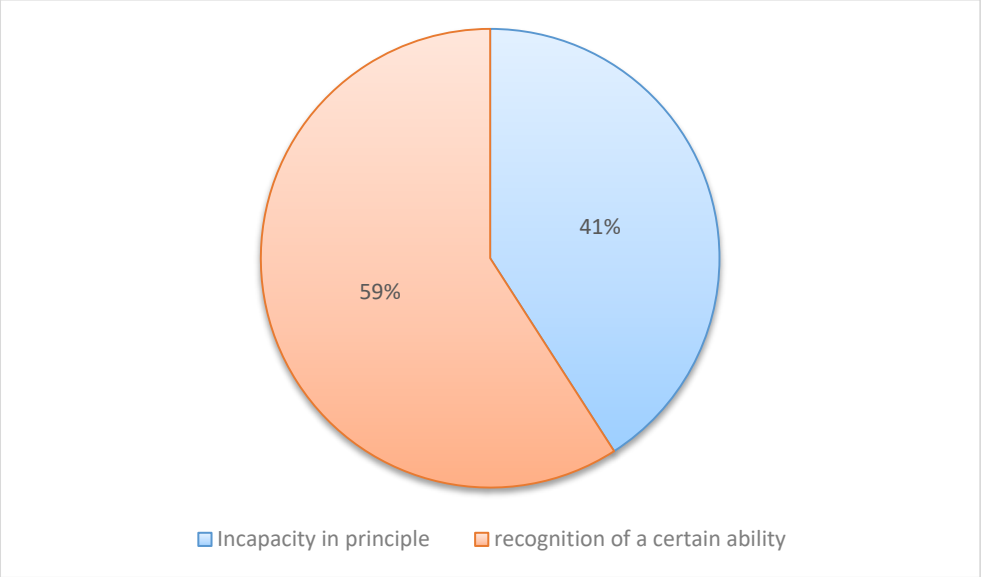
[14] FTC (2019), Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule https://beta.regulations.gov/document/FTC-2019-0054-0001:170,000 comments received, including 80,000 made public

In the United States, leading children's advocacy, health and privacy groups[15], as well as several Senators[16] 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.



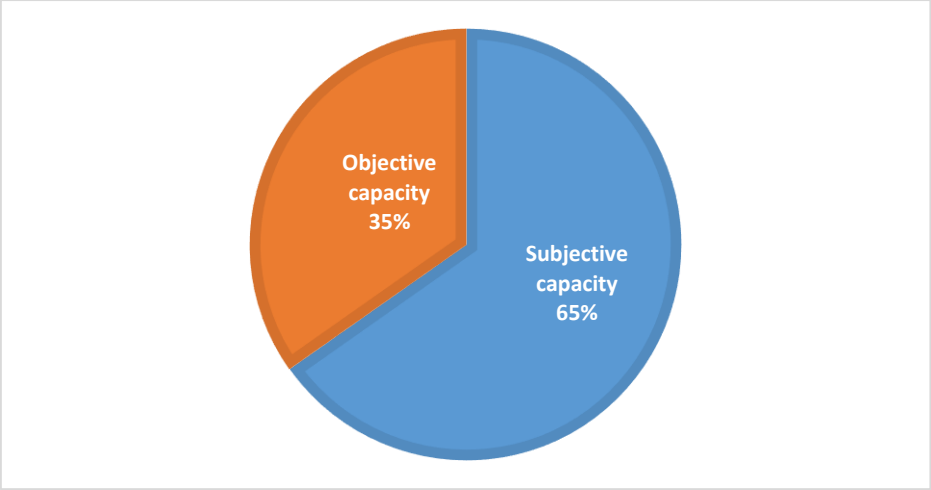
- Moreover, this trend is based in particular on an interpretation of the **letter of the data protection texts**, but also on the **International Convention on the Rights of the Child** (UNCRC).

- **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

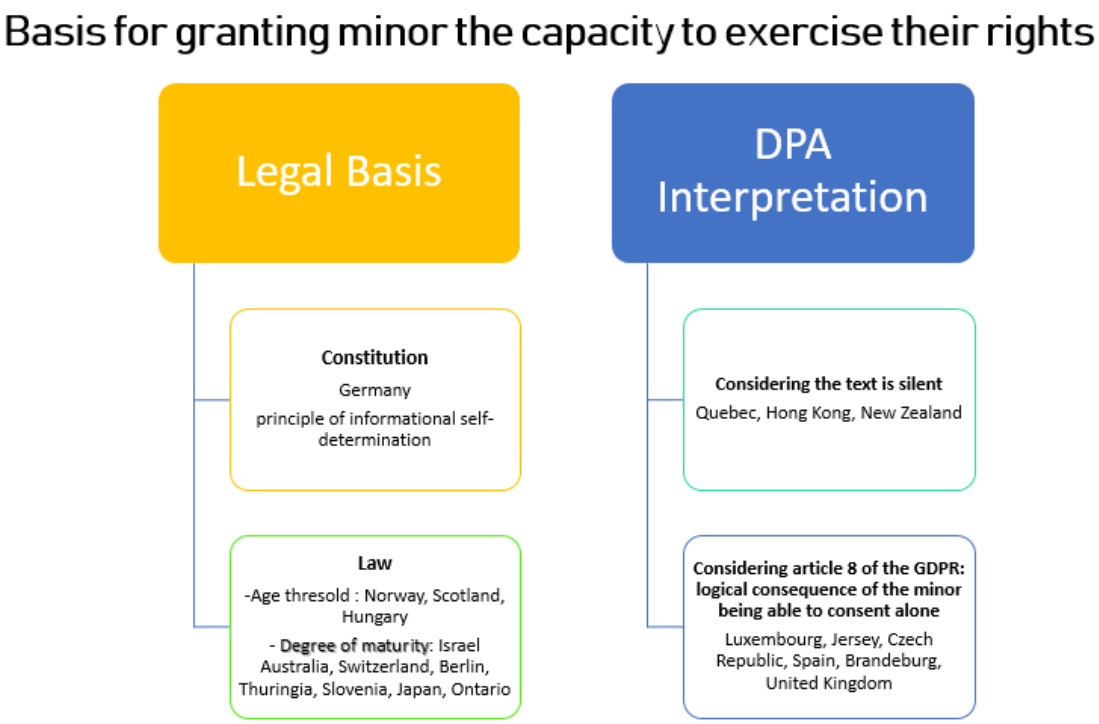
[15] Center for Digital Democracy (2019) Leading child advocacy, health, and privacy groups call on FTC to Investigate Children's Digital Media Marketplace Before Proposing any Changes to Privacy Protections for Children https://www.democraticmedia.org/article/leading-child-advocacy-health-and-privacy-groups-call-ftc-investigate-childrens-digital-0

[16] 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

their rights: 15 countries or regions have opted for the degree of maturity, and only 8 for the age threshold[17].



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



[17] 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[18]

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[19] 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**

[18] A new version has been produced [12June2020 T-PD(2019)06BISrev3].

[19] https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

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.
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**[20]. 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**.**[21]

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[22] 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 [23] 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.

---

[20] *"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.*
[21] V. recommendation 4.b on access of all children to the digital environment without discrimination
[22] OECD (2012). The Protection of Children Online https://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf
[23] 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)[24] for policy makers, industry, parents and educators, as well as children were published on 23 June 2020 by the International Telecommunication Union[25].
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[26]. At the same time, **broad consultations**

[24] Launch on 23 June 2020 https://www.itu.int/fr/mediacentre/Pages/pr10-2020-Guidelines-Child-Online-Protecion.aspx

[25] The International Telecommunication Union (ITU- COP (Children Online Protection) is the United Nations specialised agency for information and communication technologies (ICTs).

[26] 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.

with children (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**[27] . 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[28] on the right to privacy launched a call for contributions[29] 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

https://www.ohchr.org/EN/HRBodies/CRC/Pages/Submissions_Concept_GC_Digital_Environment.aspx

[27]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

[28] Prof. Joseph CANNATACI

[29] https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/CFI_Privacy_and_Children.aspx Submissions must be received by **30 September 2020**.

be given to the work, reflection and experiences of data protection authorities in relation to these issues.

2.6 UNICEF initiative

In 2018, UNICEF published a **[30]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**[31] **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[32].

[30] 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

[31] https://ec.europa.eu/research/participants/data/ref/other_eu_prog/other/pppa/wp-call/pp-call-document-pppa-agever-01-2020_en.pdf

[32] EDPS (2019) Work Program https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf