



43rd Closed Session of the Global Privacy Assembly October 2021

Adopted Resolution on children's digital rights

SPONSORS: *on behalf of the Digital Education Working Group (DEWG)*

- Commission Nationale de l'Informatique et des Libertés, France
- Garante per la protezione dei dati personali, Italy

CO-SPONSORS:

- Office of the Privacy Commissioner, Canada
- Superintendencia of Industry and Commerce, Colombia
- Personal Data Protection Office, Poland
- Commission Nationale pour la Protection des Données, Luxembourg
- Hellenic Data Protection Authority, Greece
- State Inspector's Service, Georgia
- Catalan Data Protection Agency, Spain
- Dutch Data Protection Authority, the Netherlands
- Data Inspectorate, Norway
- Information Commissioner's Office, United Kingdom
- Data Protection Agency, Spain
- Information and Privacy Commissioner, Ontario
- National Data Protection Commission, Portugal
- National Commission for the control and the protection of Personal Data, Morocco
- National Commission for Informatics and Liberties, Burkina Faso
- National Privacy Commission, the Philippines
- Office of the Privacy Commissioner for Personal Data, Hong Kong, China
- Federal Data Protection and Information Commissioner, Switzerland
- National Institute for Transparency, Access to Information and Personal Data Protection, Mexico
- Institute for Transparency, Access to Information and Protection of Personal Data, the State of Mexico and Municipalities
- Data Protection Commissioner, Council of Europe

Recalling the main international instruments in force, some of which relate to fundamental human rights and the protection of personal data and privacy:

Universal Declaration of Human Rights of 10 December 1948 - Articles 25 and 26, paragraph 3;
European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950 - Article 8;
Charter of Fundamental Rights of the European Union of 7 December 2000 - Article 24(1);
United Nations International Covenant on Economic, Social and Cultural Rights of 16 December 1966 - Article 17;
Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 and its amending Protocol "Convention 108+";
General Data Protection Regulation of 27 April 2016;
OECD Privacy Guidelines of 1980 and updated in 2013;
Montevideo Memorandum of Understanding on youth digital exclusion;

Having regard to the United Nations Convention on the Rights of the Child (CRC) of 20 November 1989 and the UN Committee on the Rights of the Child General Comment No. 25 on the Rights of the Child in relation to the digital environment of 2 March 2021,

Having regard to the European Convention on the Exercise of Children's Rights of the Council of Europe of 25 January 1996,

Having regard to the OECD Council Recommendation on Children in the Digital Environment of 31 May 2021,

Having regard to Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe to member states on Guidelines on respecting, protecting and fulfilling the rights of the child in the digital environment; Recommendation CM/Rec(2019)10 of the Committee of Ministers of the Council of Europe to member states on developing and promoting education for digital citizenship the Council of Europe Guidelines on the protection of children's personal data in an educational setting (2020); the Declaration of the Committee of Ministers on the protection of the right to privacy of children in the digital environment (2021);

Having regard to the two resolutions of the 30th International Conference of Data Protection and Privacy Commissioners in 2008, the first on privacy in social networking services and the second on children's online privacy;

Having regard to the Working Paper of the **International Working Group on Data Protection in Telecommunications, now International Working Group on Data Protection in Technology – IWGDPT, also known as “Berlin Group”**, on "Protecting the Privacy of Children in Online Services" of 9-10 April 2019, adopted at the IWGDPT's 65th meeting in Bled, Slovenia;

Affirming that children deserve special protection and as such enjoy rights recognised by the UN Convention on the Rights of the Child, in particular the right to participation (art.12) and privacy (art.16);

Highlighting that these rights are intended to apply and be deployed in all aspects of the child's life, and therefore in particular in their online life;

Recalling that, as stated in the UN General Comment on the Rights of the Child in relation to the Digital Environment (§67), privacy is essential for the empowerment, dignity and safety of children and for the exercise of children's rights;

Recalling also that minors, like any other person, have the right to informational self-determination, which implies giving them a certain autonomy and control over their personal data;

Noting that children are growing up more and more connected; that their digital practices, which have taken on an unprecedented scale with the health crisis, are widespread and increasingly autonomous;

Affirming that in a context where the impact of the digital environment on children's development, their daily lives, their future and the opportunities available to them is increasingly important, it is essential to promote respect for children's rights;

Considering that from the information that exists about minors online, their digital identity is created, which affects their present and future as human beings;

Noting that everything that is done online leaves a mark and once information is placed on the internet, control over it may be subject to be lost because it can be collected and used by third parties without one's knowledge;

Underlining that, in this context, providers of online services to which children may have access must be made aware of children having access to their services and of their increased responsibility towards minors whose personal data they process;

Affirming that in the implementation of policies relating to their rights in the digital environment, taking into account the evolving capacities of children and their best interests must be a primary consideration. Determining an appropriate balance between protecting children and accommodating their emerging autonomy is more necessary than ever to enable them to take full advantage of the digital environment while minimizing the risks to which they may be exposed;

Considering that the digital environment offers undeniable opportunities for young users: it can contribute to their education, to their access to information and leisure activities, to the formation and expression of their opinions, to the development of their personality; it enables them to maintain or develop family and social relationships;

Observing, however, that digital technologies entail risks to their privacy and intimacy as well as to their physical and psychological integrity, in that they may, in particular, confront them with cyber-bullying, online hate, and expose them to offensive or inappropriate content;

Noting that children are particularly vulnerable because they may be less aware of these risks, but also because they are a target audience for many economic actors who covet their personal data, and finally because they are sensitive to the techniques used to capture their attention, to induce them to disclose certain information, to adopt certain purchasing behaviours and to offer them personalised content;

Emphasizing that these elements call for particular vigilance with regard to respect for their right to privacy, non-discrimination and ensure their freedom of expression and opinion;

Considering that children's vulnerability must be analysed in relation to their evolving capacity to act and the subsequent need to verify with particular rigour the solidity of the contract as legal basis for the processing of children's personal data with particular reference to contracts concerning

electronic communications services; as well as in view of the possible need for further specific regulation on children's capacity to act in the digital world;

Observing the need to develop mechanisms to raise awareness among children, parents, guardians, caregivers and educators/teachers of online business practices that may cause harm to minors;

Noting that initiatives are multiplying in international organisations to strengthen the protection of the data and digital rights of minors, as evidenced by the UN's "[General Comment on the Rights of the Child in the Digital Environment](#)", the actions of [UNICEF](#), the [OECD Recommendation](#), the guidelines of the [Council of Europe](#) and of the [International Telecommunication Union \(ITU\)](#);

Observing that in parallel, several national data protection authorities have made this topic a priority, such as the "[Children's Code](#)" (formally known as the [Age-Appropriate Design Code](#)) developed by the Information Commissioner's Office (ICO), UK, the "[14 core principles for a child-centred approach to data processing](#)" established by the Irish Data Protection Commission (DPC), [the 8 recommendations to enhance the protection of children online](#) adopted by the French Data protection authority (CNIL) or the review of the Children's Online Privacy Protection Rule by the U.S. Federal Trade Commission (FTC);

Considering that the protection of children's privacy online is a priority for action in the strategic action plan of the members of the GPA; that raising awareness and training children to protect their personal data, helping them to become responsible digital citizens and to exercise their rights in accordance with the principles of parental responsibility, and safeguarding their rights in relation to parental prerogatives and rights, have been key objectives for the GPA for many years; that promoting digital education that respects the rights and freedoms of each individual is also one of its essential objectives;

Stressing that in this regard, the members of the Digital Education Working Group (DEWG) created by the resolution adopted by the ICDPPC Conference in 2013 "[Digital Education for All](#)" was mandated to "provide special protection for children in the digital world". The GPA, in this sense, has adopted several resolutions on digital education;

Observing that all these initiatives reveal a positive dynamic of awareness of the issues related to the digital practices of children, which must be pursued and encouraged, particularly as regards the promotion of children's digital rights;

Whereas these rights may provide for the possibility for the child to have access to data concerning him or her which are processed by a public authority or a private body, to have them deleted or to obtain the rectification of inaccurate or obsolete data, and also to be able to withdraw his or her consent or to object to the processing of his or her personal data;

In view of the above, **the 43rd Global Privacy Assembly calls on** all parties concerned in the field of protection of children's rights in the digital environment and recommends:

I Concerning the exercise of children's rights and information in the digital environment

- That the capacity of children to exercise their digital rights directly be expressly affirmed: it is important to emphasize that these rights are recognised as belonging to individuals and that as such they fundamentally belong to children themselves; consequently, when parents or legal guardians exercise these rights on behalf of the child, they must do so in consideration

of guiding principles of the UN CRC, including the child's best interests alone, the right to development, non-discrimination and the right to be heard ;

- That in order to assert one's rights one must first know them: that in this sense the realisation of children's digital rights implies informing children, as well as their parents and teachers, about their content and how to exercise them; that this information must be presented to children in clear and tailored language and a way that is adapted to their age and capacity for understanding, at the time when the data is first used but also accessible at all times and presented in such a way as to encourage children to learn more about their rights in the digital environment;
- That the appropriate information to be given to children should also cover the way in which their data is processed: in this respect, **online service providers** should post a privacy policy as well as clear and simple terms and conditions of use (TOU), but also publish a list of their commitments to child data protection, to which they should strive to adhere to, such as age restrictions and behaviour rules;
- That **States** should consider encouraging at the national level the creation and distribution of updated and age-specific educational resources to raise awareness among children, youth, parents, educators/teachers and schools about digital rights and how to exercise them in practice on social media platforms and networks or through complaint procedures, content deletion and reclaiming mechanisms that are accessible and appropriate for children;
- That the effectiveness of rights is also conditioned by the existence of rapid, accessible, and appropriate remedies that are also available for children with **data controllers** and **data protection authorities**;
- That **Controllers and Data Protection Authorities** should consider implementing child-friendly complaints processes, which ought to be easily accessible and reasonable to fill in;
- That all these elements call for particular attention to be paid to the design of interfaces, which is the cornerstone of information, digital rights and the quality of consent given by the data subject; in particular, **online service providers** should not incorporate manipulation and deceptive design techniques (*dark patterns or nudge techniques*) that would influence children to take decisions that would unduly affect their privacy or provide more personal data than is necessary;
- That minors should be also aware that in the digital environment it is important to respect the rights of others;

II Concerning the protection of children's fundamental freedoms with regard to the processing of their personal data

- That the promotion of the autonomy of children and the protection of their informational self-determination invites, as recalled by the UN Committee on the Rights of the Child General

Comment (§71), to ensure the free and informed nature of the consent given by the child, or, depending on his or her age and evolving capacities, by the parent or legal guardian, who should always seek to involve the child in this expression of will;

- That, in line with these same UN observations, the tracking of children made possible by digital technology must respect the child's right to privacy: As such, it must be off by default; where necessary, it must not be systematic or carried out without the knowledge of the child or, in the case of young children, their parents or carers; the person concerned must always be able to object to such tracking, whether on commercial premises or in educational and care facilities, and the least privacy-invasive means possible should always be considered to achieve the desired objective;
- That age assurance mechanisms that may be put in place to protect children from inappropriate content or to perform certain acts online must respect their privacy. The design, development and implementation of such systems **by online service providers** should be based on a risk assessment, be in line with data protection principles, including privacy by design, the principle of data minimisation, purpose limitation, and ensuring the least intrusive method is adopted; an internationally harmonised approach should be worked out in this area;
- That **States** should consider introducing regulations which prohibit practices which manipulate children or which aim to unduly influence their behaviour and, in particular in a way which may be against their best interests: that profiling and automated decision-making may also undermine children's right to non-discrimination and their ability to freely form and express their views in the digital environment; that the need for this change in the legal framework is all the more pressing as these technologies can be used to influence children's behaviour and emotions in contexts where the child is vulnerable, such as in education, health or criminal justice areas;
- That **Controllers and Processors** implement accountability measures of reinforced responsibility which imply among others greater measures of security and those preventing unauthorized consultation, use, or access;

III Concerning the protection of children against the commercial exploitation of their data

- That **States** should consider promoting regulations prohibiting the use or transmission to third parties of children's data for commercial or advertising purposes and the practice of marketing techniques that may encourage children to provide personal data;
- When children contract with Electronic Communications Services, the service providers should only process children's basic information such as name, account and other technical data strictly necessary for the use of the services, **States** should also consider introducing legislation in this regard taking into account age threshold and/or level of maturity.

- That **controllers** and **online service providers** refrain from profiling children on the basis of a digital record of their actual or presumed characteristics for commercial purposes, and even avoid any dissemination or disclosure of personal data of an informative or newsworthy nature to the public or of a newsworthy nature which would enable them to be identified and which would be detrimental to their honour, image or reputation.

IV Concerning the inclusion of children's views and rights in the development of regulations and the design of services that affect them

- That the participation of children is largely promoted in the development of public policies that concern them through processes of consultation and co-construction of the solutions that will be proposed to them, involving them in a manner appropriate to their age and the development of their capacities;
- That **online service providers** should integrate the promotion of the best interests of the child and respect for children's rights into the design of services: in this sense, they should provide for the use of privacy impact assessments, children's rights impact assessments, data encryption solutions, easy-to-understand and easy-to-use privacy settings and default settings that offer the highest protection of children's personal data, and in particular the deactivation by default of certain options, such as geolocation and profiling; and they should also consult with children, parents, or child advocates during the development of their services.
- That **States** should consider assessing the impact on children's rights, including from a human rights perspective, of any legislation relating to the digital environment and in the design of online services that children may access;
- That **States and online service providers, with the support of data protection authorities**, should encourage the implementation of industry codes and terms and conditions of service that meet the highest standards of ethics, privacy and child safety in all stages of the value chain, including design; as well as the introduction of contractual provisions about the limitation of use of personal data further than basic information strictly necessary for the use of the services;
- That the certification of products and/or services should be promoted to ensure that the processing is carried out in compliance with current laws on privacy and personal data protection;

V Concerning the involvement of the holders of parental authority and digital education

- That **States, in cooperation with data protection authorities**, should consider setting up educational programmes, actions and awareness campaigns for children, parents, education-providers, the general public, political decision-makers and companies in order to improve their knowledge of the challenges, opportunities and risks linked to the digital practices of children, as well as the rights of the child in the digital environment;

- That **States** should encourage those responsible for the processing of personal data in both the public and private sectors to work closely with parents and guardians of children and adolescents, either through participatory democracy exercises or by drafting charters for digital rights tailored to the specific needs of the children's rights sector.
- That the development of awareness-raising campaigns that help minors to inform parents, guardians, teachers, or a trusted adult if they feel in danger online or if other minors might be in danger online, will be carried out;
- That in such campaigns, parental commitment that respects the interests and privacy of the child should be fostered, which implies technically providing for parental consent when legally required, but also ensuring that the parental control devices proposed comply with data protection rules, and in particular respect the principle of transparency towards the child, with the child being aware of parental control and tracking devices, the principle of proportionality, which should lead to avoid the use of intrusive devices or features such as excessive tracking, and a principle of security of the child's data towards third parties;
- That **States** should consider promoting, in consultation with **the data protection authorities, children, other public actors and the operators concerned**, an evaluation of the parental control devices proposed on the market and their compliance with data protection rules;
- That **States** should consider providing sufficient human and financial resources, in particular to assess the impact of public policies implemented in the field of digital citizenship education, as well as adequate training for educational professionals so that these programmes, actions and campaigns can effectively raise the awareness of the public for whom they are intended;
- That **States and the data protection authorities** should develop, where appropriate, these activities in collaboration with institutional and associative committed stakeholders for children's rights in the digital environment, in order to amplify the impact of these actions and to benefit from adapted and diversified skills and knowledge;
- That cooperation mechanisms between **data protection authorities and also with the Digital Education Working Group** should be strengthened in order to exchange best practices related to the exercise of children's digital rights, to improve regulatory actions concerning them and as a follow up to this Resolution;
- That **the data protection authorities** should promote this Resolution and its recommendations to stakeholders and policy makers in their jurisdictions and networks.

Explanatory note

The digital environment is particularly important to provide opportunities to children, but the digital sphere entails particular risks of infringement of their rights, and in particular their right to privacy. Children's rights are meant to be realised in all aspects of the lives of contemporary children, and therefore also in their online lives.

For this reason, protecting children's privacy online is a priority for action in the strategic plan¹ of the Global Privacy Assembly membership (GPA), which adopted several resolutions on digital education initiated by the Digital Education Working Group (DEWG).²

In view of the need to provide more information to children, as well as their parents and educators, about their rights in order to guarantee their effectiveness, the Digital Education Working Group conducted successive surveys in 2019 and 2020 aimed at taking stock of the existing legal framework in the different States concerning the exercise of their rights by minors, and in particular their privacy rights. The survey results of the study, published in September 2020³, was based on a panel of 46 data protection authorities, and found out that there are legal provisions in countries that allow children to exercise their privacy rights. However, the framework remains relatively unclear as to who, children or parents on their behalf, can exercise these rights - bearing in mind the notions of digital maturity and legal capacity of children.

At the same time, the DEWG has been actively monitoring with its GPA members various national and international initiatives and revised policy guidelines that may shed new light on the issue of children's rights.

Likewise, we strongly believe that this Resolution on children's digital rights ought to have a major impact around the world since it will convey the message that determining an appropriate balance between protecting children and accommodating their emerging autonomy is - in the current pandemic crisis- more necessary than ever to enable all of them to take full advantage of the digital environment while minimizing the risks and harms to which they may be exposed.

As a follow-up to the implementation of this resolution, the DEWG will consult its members to consider whether the exercise of digital rights in practice by children themselves, or by their legal representatives via online services, is easily accessible and understandable, and will evaluate compliance with and the effectiveness of the measures listed to support all stakeholders concerned.

All the priority issues arising from the resolution should be reflected in the GPA's 2021-2023 Strategic plan to be discussed and submitted for adoption at the 43rd Global Privacy Assembly. To this end, all GPA working groups should examine the issue of child protection and the exercise of their digital rights that are relevant to their area of work and include them in their annual forward plan, as appropriate, and in coordination with the DEWG which is primarily tasked with examining it.

¹ [GPA Strategic Plan](#) (see page 9)

² [Resolution on Digital Education for All \(2013\)](#)
[Resolution for the Adoption of an International Data Protection Education Benchmark \(2016\)](#)
[Data Protection Training Framework for Students \(2016\)](#)
[Resolution on e-learning platforms \(2018\)](#)

³ [Legal framework and practices of data protection authorities regarding the exercise of minors' rights](#)