COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 17 November / novembre 2020

T-PD(2019)06BISrev3Com/Mos2

**CONSULTATIVE COMMITTEE OF THE
CONVENTION FOR THE PROTECTION OF INDIVIDUALS
WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA**

**COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION
DES PERSONNES A L'ÉGARD DU TRAITEMENT AUTOMATISÉ
DES DONNÉES A CARACTÈRE PERSONNEL**

CONVENTION 108

COMPILATION OF COMMENTS / COMPILATION DES COMMENTAIRES

Children's Data Protection in an Education setting

La protection des données personnelles des enfants dans un cadre éducatif

Directorate General of Human Rights and the Rule of Law

Direction Générale droits de l'Homme et Etat de droit

TABLE OF CONTENTS / TABLE DES MATIÈRES

GERMANY / ALLEMAGNE

The expansion of educational technology means non-state actors routinely control children's educational records not only in independent schools, but also in 'public' or 'state' schools. The digital infrastructure to deliver state education is often commercially owned. This can introduce new questions of where control of the curriculum sits if content type and delivery is shaped by the technology platform, and questions of security and sustainability.

Companies can lock in schools to proprietary software practices, with consequences for interoperability, for data access and reuse, and the budgetary and environmental impacts of obsolescence, for example where a company decides to discontinue hardware or software upgrades. It is common, at the time of writing, for small companies to be incubated by angel investors and later be bought out by other larger companies. Controllership and storage of personal data can thus be transferred in takeovers multiple times over, in the course of a child's education.

Children cannot see or understand how large their digital footprint has become or how far it travels to thousands of third parties across or beyond the education landscape, throughout their lifetime. While children's agency is vital and they must be better informed of how their own personal data are collected and processed, there is at the same time a consensus that children cannot be expected to understand a very complex online environment and to take on its responsibilities alone.

5.3. The right to be heard

5.3.5. Data processing on the basis of consent, which must be freely given, specific, informed and unambiguous ~~may be invalid~~ where a power imbalance exists, notably between a public authority and an individual. This imbalance is even more significant where the data subject is a child. Another basis is therefore more likely to be valid for routine processing activities and such processing should be based in law.

7.1. Legitimacy and lawful basis

7.1.7. Children should not be expected to enter into a contract with third parties, for example with an e-learning provider or application mandated by the educational setting. ~~The educational setting should process children's data on the basis of a written contract between *the* setting and the third party~~. Personal data processing by such services should be carried out on a legitimate basis laid down by law.

7.1.12. ~~Controllers and processors shall not give away children's personal data collected in the course of their education, for others to monetise, or reprocess it for the purposes of selling anonymised or de-identified data, for example to data brokers.~~

7.5. Securing personal data in an Education Setting

7.5.9. Where encryption is not integrated into an application or service, it may be appropriate to encrypt data "manually" ~~as~~ stand-alone protective measure.

8.1. Standards

8.1.2. Standards may be set out in Codes of Practice and certification which should be drafted on the basis of a wide cooperation with developers and industry, with education practitioners, academia, with organisations representing teachers and families, and civil society and with children themselves.

ITALY / ITALIE

1. Introduction

The sensitivity of digitised pupil and student data should not be underestimated, as the International Working Group on Data Protection in Telecommunications set out in the Working Paper on e- learning platforms in 2017. “Some of these e-learning platforms and the learning analytics they facilitate have enormous capacity to foster the development of innovative and effective learning practices. At their best, they can enhance and complement the interactions of students, parents and educators in the educational environment and help them fulfil their respective potential. Nevertheless, e-learning platforms may pose threats to privacy arising from the collection, use, reuse, disclosure and storage of the personal data of these individuals.”6

3. Definitions for the purposes of the Guidelines

j. “Profile” refers to a set of data characterising a category of individuals that is intended to be applied to an individual.

k. “Profiling” means an automatic data processing technique that consists of applying a “profile” to an individual, particularly in order to take decisions concerning them or for analysing or predicting their personal preferences, behaviours and attitudes.[108]

4. Principles of data processing

Convention 108+ lays down principles, obligations and rights which apply to any processing of personal data, and are therefore essential to apply in an educational setting.

4.1. Legitimacy of the processing, and the principles of lawfulness, fairness, necessity, proportionality, purpose limitation, accuracy, limited time retention in identifiable form, transparency and data minimisation and to

[8] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805cdd00

ensure that personal data are adequate, relevant and not excessive in relation to the purposes for which they are processed.

4.2. A precautionary approach and a strengthened protection towards sensitive, special categories of data, including genetic and biometric data, and ethnic origin, or relating to sexual orientation, or offences, recognising children's additional vulnerability.

4.3. Meaningful transparency of data processing recognising the importance of accessibility through the use of clear language, in child-friendly terms and formats when appropriate, in communication, offline or online, and on any device.

4.4. Accountability of data controllers and data processors, must be clearly set out in any contractual arrangements, defined by the nature of the processing.

4.5. Privacy and data protection by design principles, and suitable organisational and technical measures, should be applied in practice.

4.6. Assessment of the likely impact of the intended processing on the rights and freedoms of the data subject prior to the commencement at the start of any data processing and across its life cycle. Particular attention needs paid at an early stage, as to how communication about data processing will be maintained, between the data controller and the child or their legal guardian, after the child has left the educational setting.

4.7. Security measures[11] are necessary to prevent and protect against risks, such as accidental or unauthorised access to, destruction, loss, misuse, modification, ransom attacks or disclosure of personal data. The growth of cloud-based and transborder data flows in educational data systems means security practices require particular attention.

4.8. Specific to educational the educational context, data controllers must recognise the rights of legal guardians to act on behalf of and in their child's best interests in accordance with domestic and international law. Best effort should be made to involve a child in decisions about them and provide suitable information to families, where

5.3. The right to be heard

5.3.3. Legal guardians and children should both be informed where data processing requires that information is processed fairly in accordance with Article 5(4)(a), of the Convention 108+ unless sharing such information poses a risk to the best interests of the child, with due regards to Article 11(b) of the Convention, or unless a competent child makes an objection to the involvement of one or more legal guardian.

5.3.4. In accordance with States Parties 'law, including taking into account any age limits set out in law for consent to data processing by information society services (ISS) where the definition of an ISS is applied in an educational setting, and to support the child as data subject, legal guardians should be permitted to exercise rights under Article 9 (1)(b) of Convention 108+, on behalf of the child in education, where the child does not object, taking into account their level of capacity and the best interests of the child.

5.3.5. Data processing on the basis of consent, which must be freely given, specific, informed and unambiguous may be invalid where a power imbalance exists, notably between a public authority and an individual. This imbalance is even more significant where the data subject is a child. Another basis is therefore more likely to be valid for routine processing activities and such processing should be based in law.

5.3.6. Children should be enabled by provision of child-friendly, transparent, comprehensible and
accessible information on the data processing to both give and withhold consent where they
have the capacity to understand the implications, and processing is in their own best
interests, and in line with any age based laws in domestic and international legislation.

5.3.7. Children should have the right to access appropriate, comprehensible, independent and
effective complaints mechanisms and exercise their rights.

6.1. Review legislation, policies and practice

6.2. Offer effective support for children's rights to be heard

.

6.2.2. Representation of child data subjects to supervisory authorities (Article 18) by third parties should be accessible and strengthened. States Parties may provide under Article 13 for extended protection in their legislation. It should be made possible that any body, organisation or association independently of a data subject's mandate, has the right to lodge a complaint with the competent supervisory authority, in that State Party, where permitted by Member State law, if it considers that the rights of a data subject have been infringed as a result of processing.

7. Recommendations for data controllers

There are many actors in the data processing chain who may be data controllers; not only educational institutions and government bodies, but providers of platforms, devices, programmes and applications. The latter commercial actors may also be data controllers in their own right, where they alone or jointly with others determine the nature of the processing as defined in Article 2 of the Convention 108+ and careful attention is needed to understand that the nature of the processing determines each role and not solely what is set out in contract terms. The obligations upon data controllers may not always fall solely on the educational setting as a result. To meet all the relevant data protection principles including data accuracy, necessity, and security; educational settings need to encourage a good data governance culture in which risk assessment proactively considers rights and freedoms as part of any processing or procurement process and data quality is proactively monitored and effectively managed through records management, supported by skills training, and policies.

7.1. Legitimacy and lawful basis

7.1.3. A child's special category of data, as defined in Article 6, requires enhanced protection when being processed, starting with the appropriate legal basis for the processing. Where there is no other lawful basis for processing, informed and freely given consent should be obtained from a legal guardian for the processing of health and other special categories of data, and recorded as an appropriate safeguard under Article 6(1) for a child, when processing is in the best interests of the child. Such data may be shared for purposes that go beyond their direct

care and education, only with freely given, specific, informed and explicit consent of the data subject or their legal guardian.

7.2. Fairness

7.2.1. Article 8(1)(e) of the Convention 108+ requires any data processing to be transparent, and complete and as set out in the Explanatory Report of the Convention 108+, that means in a way that can be fairly and effectively presented to a data subject, for example, according to the child's evolving capacity and in a child-friendly, comprehensible language and accessible alternative formats to text-only where appropriate in accordance with paragraph 68 of the Explanatory Report of the Convention. It should be interpreted in the educational context as necessary to be understood by a child according to their capacity, or by their legal guardians.

7.5. Securing personal data in an Education Setting

7.5.1. The protective measures applied to personal data should be based on a risk assessment following industry standards and best practice, and using established guidance (such as ISO 17799:2000).

7.5.2. Applicable controls are likely to be a combination of authentication, authorisation and access control measures, and may be a combination of digital and non-digital measures.

7.5.3. The following factors should be considered:

- Physical accessibility (e.g. to devices and data in the education setting)
- Networked access to devices and data
- Backup and archival of data

7.5.4. Physical accessibility includes data collected or stored in at least the following contexts:

- Classroom/e-learning (including distance learning outside school premises)
- School administration
- Premises (physical access, CCTV including on school vehicles, biometric readers)

7.5.6. For networked access to data, authentication is almost certain to be required, and is desirable, to prevent unauthorised access. The same questions arise as for on-site access: what is the most appropriate authentication

technology, and is access granted on the basis of individual identity (firstname.lastname) or an attribute ("pupil at this school").

7.6. Automated decisions and profiling

7.6.1. Every individual has the right not to be subject to a decision significantly affecting them, based solely on an automated processing of data without having his or her views taken into consideration. Knowledge of the reasoning underlying the data processing where the results are applied to the data subject, should be made readily available, in accordance with Article 9(1)(a) and 9(1)(c) of Convention 108+.

7.6.9. The distribution and use of software or use of services designed to observe and monitor user activity on a terminal or communication network building a profile of behaviour should not be permitted, unless expressly provided for by domestic law, and accompanied by appropriate safeguards, as set out in Principle 3.8 of Council of Europe recommendation CM/Rec(2010)13 and explanatory memorandum[239], on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

7.7.3. The use of biometrics in educational settings such as for identity verification including remote proctoring, shall only be allowed where no less invasive method may achieve the same aim, and with appropriate safeguards enshrined in law, in accordance with Article 6(1) of Convention 108+. This should include due regard for the risks that the processing of sensitive data may present for the rights and fundamental freedoms of the child, including lifelong discrimination. Alternative methods should be offered without detriment.

7.7.5. Educational settings should pay particular attention to where their use of a service constitutes a contractual agreement, for example in the use of videoconferencing software in order to be able to implement distant learning programs, and in which staff may agree to terms-and- conditions of service that include the processing and recording of content including children's images and voice data. Staff should ensure that where data processing is on the basis of consent, that consent cannot be assumed by the education setting and granted on behalf of the child, but must be freely given by the data subject, the child in accordance with their evolving capacities or their legal guardian.

8. Recommendations for industry cooperation

8.3. Design features with data protection and privacy implications

[9] Council of Europe recommendation CM/Rec(2010)13 and explanatory memorandum (2011) https://rm.coe.int/16807096c3

8.3.5. Specific attention should be given to Article 14 under the Convention, to make sure transborder flows of personal data for the purposes of education meet the conditions of the article, to limit transborder flows of personal data for the purposes of education, and to ensure that transborder flows take place within a recognised data protection framework and within domestic law.

SWEDEN / SUÈDE

1. Introduction

~~Stakeholders should collaborate to create a rights-respecting environment, to uphold Article 8 of the European Convention on Human Rights and protect the human dignity and fundamental freedoms of every individual, in respect of data protection.~~

The introduction of digital tools to the classroom in effect opens up the school gates to a wide range and high volume of stakeholders who interact with children's everyday activities. The majority of the devices and applications, software and learning platforms, adopted in educational settings are developed by private, commercial actors.

Stakeholders should collaborate to create a rights-respecting environment, to uphold Article 8 of the European Convention on Human Rights and protect the human dignity and fundamental freedoms of every individual, in respect of data protection.

Much commercial software in education is known as‘ freeware’~~,~~ software offered to educational settings at no direct financial cost. According to the EU e-commerce Directive (Art 1.1) this would generally fall within the definition of an Information Society Service[10] "provided for remuneration", ~~often in a non-explicit exchange for~~ where the personal data processed about the user in exchange for the service must be understood as a kind of remuneration.

The expansion of educational technology means non-state actors routinely control children's educational records not only in independent schools, but also in 'public' or 'state' schools.

The digital infrastructure to deliver state education is often commercially owned. This can introduce new questions of where control of the curriculum sits if content type and delivery is shaped by the technology platform, and questions of security and sustainability. ~~Companies can lock in schools to proprietary software practices.~~ Schools must be aware of and properly manage that proprietary software practices may cause lock-in effects, with consequences for interoperability, for data access and reuse, and the budgetary and environmental impacts of obsolescence, for example where a company decides to discontinue hardware or software upgrades. It is common, at the time of writing, for small companies to be incubated by angel investors and later be bought out by other larger companies. Controllership and storage of personal data can thus be transferred in takeovers multiple times over, in the course of a child's education.

Children cannot see or understand how large their digital footprint has become or how far it travels to thousands of third parties across or beyond the education landscape, throughout their lifetime. While children's agency is vital and they must be better informed of how their own personal data are collected and processed, there is at the same time a consensus that children cannot be expected to understand a very complex online environment and to take on its responsibilities alone.

[10] To determine the scope of the term 'information society service" in the GDPR for example, reference is made in Article 4(25) GDPR to Directive 2015/1535. See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 (para 128).

The investigative burden needed before procuring products or services in educational settings can make it hard even for adults to fully understand software tools and their processing;, including assessing the comparative implications of using open or proprietary information and communication technology ICT, paid-services or freeware or to carry out adequate risk assessment, and to retrieve and offer the relevant information required to provide to the data subject. This makes it hard to s, and be ablesufficiently qualified to meet and uphold users 'rights, including the comparative implications of using open or proprietary ICT, paid-services or freeware.

Recognising that legislation on educational settings and other domestic and international law has an impact on how the data protection rules are applied, including the rights of data subjects, eEducational institutions need strong legislative frameworks and Codes of Practice to empower staff, and to give clarity to companies to know what is permitted and what is not, when processing children's data from educationin the context of educational activities, creating a fair playing field for everyone.

StakeholdersPolicy makers and practitioners, including legislators, supervisory authorities in accordance with Article 15 (2)(e) of the Convention 108+, and policy makers, educational authorities and industry, should follow and promote these Guidelines and implement measures to meet data protection and privacy obligations.

Materials should also be made available to children and their representatives, in a child-friendly and accessible manner.

This is especially relevant inIn educational settings , where children are disempowered in their relationship with a public authority and are also recognised as vulnerable due to their lack of understanding and capacity, disempowerment, and state of being in the process of development into adulthood. From the static point of view the child is a person who has not yet attained physical and psychological maturity. From a dynamic point of view, the child is in the process of developing to become an adult. (Working Party 29, 2009).[11] Children are also active rights holders, and agents who require not only protection but also provision of information, training, and guidance.

Materials such as informational guides and fair processing documents, should also be made available to children and their representatives, in a child-friendly and accessible manner.

[11] Working Party 29 Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf 5 Working Paper in English: Working Paper on E-Learning Platforms (Washington D.C.

These guidelines should also apply wherever remote e-learning solutions are engaged as the result of a child's enrolment at an educational setting and aare used outside the educational setting such as for homework or distance learning. Distance learning tools and resources should be subject to the same rigorous due diligence for pedagogical quality, safety and data protection standards, for instance regarding the default settings, so that the usage of applications and software does not infringe the rights of the data subjects (data protection by default). Processing must not involve more data than necessary to achieve the legitimate purpose. Thislt is particularly important when consent is not possible to be freely given, when the choice is to use a product and receive remote instruction, or not and receive none.

When a school requires the use of e-learning tools, a consent basis for processing personal data either by the school or by the third party processor will not be valid, because any consent required by companies must be freely unambiguously freely given and able to be refused without detriment.[12] and valid, and educational settings and companies must seek another lawful basis for processing where consent cannot be freely given, or be refused without detriment. That may mean companies need to reduce their own processing purposes, to meet only those purposes that are necessary and proportionate, from the perspective of the school in its public task remit.

It is important to remember that the data protection rules are not applied in isolation from the legislation on educational settings or law on equality, employment, privacy of communications and other relevant and domestic law.

The guidelines should be applied together with the existing principles of data protection highlighted in section three, including the principle of data minimisation.

Today's aAdults should ensure that protections offered to children are not only appropriate for the duration of their childhood, but also consider theirchildren's future interests. We have a duty to promote the ability of children to reach maturity unimpeded, and able to develop fully and freely, to meet their full potential and foster human flourishing.

I. Scope and Purpose

2. The Guidelines aim to ensure that the full range of the rights of the child are met as pertains to data protection in and as a result of interactions with an educational setting, among which isare the rights to information, to representation, to participation, and to privacy. They should be fully respected and given due consideration for the child's level of maturity and understanding.

[12] In this context, it should also be taken into account that recital 43 of the GDPR states that "in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is *a clear imbalance between the data subject and the controller*, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation" and that children in an educational setting constitute a typical example of a situation where there is an imbalance between the data subject and the controller and where another legal basis should rather be applied.

3. Nothing in the Guidelines shall be interpreted as precluding or limiting the provisions of the European Convention on Human Rights and of Convention 108[13]. or REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). These Guidelines also take into account the new safeguards of Convention 108+.

4. The Guidelines remain high-level with a focus on legal requirements and obligations. Supervisory authorities may wish to address practical suggestions for educational settings including check-lists for those that want to integrate digital technologies in their processes as part of domestic Codes of Practice and practical guidance specific to State Parties law. States should may develop evidence-based standards and guidance for schools and other bodies responsible for procuring and using educational technologies and materials to ensure these deliver proven educational benefits and uphold the full range of children's rights.

II. Definitions for the purposes of the Guidelines

(a) "child" means every human being below the age of 18 unless the age of majority is attained earlier under the national law;

(b) "data analytics" refers to personal data used in the computational technologies that analyse large amounts of data to uncover hidden patterns, trends and correlations and refers to the whole data management lifecycle of collecting, organizing and analysing data to discover patterns, to infer situations or states, to predict and to understand behaviours.

(c) "digital environment" is understood as encompassing information and communication technologies (ICTs), including the Iinternet, mobile and associated technologies and devices, as well as digital networks, databases, contentapplications and services;

(g) "legal guardians" refers to the persons who are considered to be the parents ofhold parental responsibilities for the child according to national law and have parental responsibilities; have the collection of duties, rights and powers, which aim to promote and safeguard the rights and welfare of the child in accordance with the child's evolving capacities.

[13] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

(h) "learning analytics" can be described as the measurement, collection, analysis and reporting of data about learners and their contexts, for the purposes of understanding and optimising learning and the environments in which it occurs.[14]

(i) "processing" means any operation or set of operations performed on personal data, such as but not only the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure or destruction of, or the carrying out of logical and/or arithmetical operations on such data;

(j) ~~"profiling" refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;~~"Profile" refers to a set of data characterising a category of individuals that is intended to be applied to an individual.

(k)"Profiling" means an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take decisions concerning them or for analysing or predicting their personal preferences, behaviours and attitudes.[15]

III. Principles of data processing

Convention 108+ lays down principles, obligations and rights which apply to any processing of personal data, and are therefore essential to apply in an educational setting:

1. Legitimacy of the processing, and the principles of lawfulness, fairness, necessity, proportionality, purpose limitation, accuracy, limited time retention in identifiable form, transparency and data minimisation~~.~~ and to ensure that personal data are adequate, relevant and not excessive in relation to the purposes for which they are processed.

2. A precautionary approach and a strengthened protection towards sensitive, special categories of data, including genetic and biometric data, and ethnic origin, or relating to sexual orientation, or offences, recognising children's additional vulnerability.

[14] Learning and Academic Analytics, Siemens, G., 5 August 2011 http://www.learninganalytics.net/?p=131

[15] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168056cdd00

3. Meaningful transparency of data processing recognising the importance of accessibility through the use of clear language, in child-friendly terms and formats when appropriate, in communication, offline or online, and on any device.

4. ~~The a~~Accountability of data controllers and data processors, ~~to~~must be clearly set out in any contractual arrangements, defined by the nature of the processing.

5. Privacy and data protection by design principles, and suitable organisational and technical measures, should be applied in practice.

6. A~~n a~~ssessment of the likely impact of the intended processing on the rights and freedoms of the data subject prior to the commencement at the start of any data processing and across its life cycle. Particular attention needs paid at an early stage, as to how communication about data processing will be maintained, between the data controller and the child or their legal guardian, after the child has left the educational setting.

7. Security measures[16] are necessary to prevent and protect against risks, such as accidental or unauthorised access to, destruction, loss, misuse, modification, ransom attacks or disclosure of personal data. ~~The growth of cloud-based and transborder data flows in educational data systems means security practices require particular attention.~~

8. Specific to the educational context, data controllers must recognise the rights of legal guardians to act on behalf of and in their child's best interests in accordance with domestic and international law. Best effort should be made to involve a child in decisions about them and provide suitable information to families, where appropriate. ~~Recognition of the rights of the child in an algorithmic decision-making context, in particular associated with processing personal data using artificial intelligence (see the Guidelines on data protection and artificial intelligence)[17] .~~

~~Security measures[18] are necessary to prevent and protect against risks, such as accidental or unauthorised access to, destruction, loss, misuse, modification, ransom or disclosure of personal data. The growth of cloud-based and transborder data flows in educational data systems, means security practices require particular attention.~~

[16] Suggested reference on security of personal data during remote learning – UODO's guide for schools https://uodo.gov.pl/en/553/1118

[17] Guidelines on Artificial Intelligence and Data Protection, document T-PD(2019)01, available at https://rm.coe.int/2018-lignes-directrices-sur-l-intelligence-artificielle-et-la-protecti/168098e1b7

[18] Suggested reference ~~areas~~ on security of personal data during remote learning – UODO's guide for schools https://uodo.gov.pl/en/553/1118

IV. Fundamental principles of children's rights in an educational setting

A. *The best interests of the child*

2. In assessing the best interests of a child, States should make every effort to ~~balance, and~~balance and reconcile a child's right to protection with other rights, in particular the right to freedom of expression and information, and ~~privacy and~~ participation, as well as the right to be heard.

B. *The capacity of a child*

1. The capacities of a child ~~develop~~evolve from birth to the age of 18. Individual children reach different levels of maturity at different ages.

C. *The right to be heard*

1. Children have the right to express themselves freely in all matters affecting them, and their views should be given due weight in accordance with their age and maturity. States should make sure that children are aware of their rights in the digital environment in a child-friendly, transparent, comprehensible and accessible way. ~~specifically as regards~~Everyone in the education system ~~and~~ should ~~implement measures to~~ ensure ~~that they~~children are able to access mechanisms for enforcing their rights.

2. Staff in e~~Stakeholders~~ducational settings should establish a default position of good practice to involv~~ing~~e legal guardians and children, according to their capacity, in consultation about decisions to adopt new technology that result in ~~before~~the processing of ~~their~~ children's personal data, to ensure ~~personal data shall be processed fairly and in a transparent manner~~ a fair balance of all interests concerned, aligned with Article 5(41)~~(a),~~ of the Convention 108+. States should also ensure that consultative processes are inclusive of children who lack access to technology[19] at home.

3. Legal guardians and children should both be informed where data processing requires that information is processed fairly in accordance with Article 5(4)(a), of the Convention 108+ unless sharing such information poses a risk to the ~~child's~~ best interests of the child, with due regards to Article 11(b) of the Convention, or unless a competent child makes an objection to the involvement of one or more legal guardian.

[19] United Nations Committee on the Rights of the Child, Draft General Comment on children's rights in relation to the digital environment, August 2020 https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en

4. In accordance with States Parties' law, including taking into account any age limits set out in law for consent to data processing by information society services (ISS) where the definition of an ISS is applied in an educational setting, and to support the child as data subject, legal guardians should be permitted to exercise rights under Article 9 (1)(b) of Convention 108+, on behalf of the child in education, where the child does not object, taking into account their level of capacity and the best interests of the child.

   a. Data processing on the basis of consent, which ~~has to~~must be freely given, specific, informed and unambiguous ~~is particularly questionable~~may be invalid where a power imbalance exists, notably between a public authority and an individual. This imbalance is ~~even more so the case~~even more significant where the data subject is a child. Another ~~lawful~~ basis is therefore more likely to be valid for routine processing activities and such processing should be based in law.~~.~~

   b. Children should be enabled by provision of child-friendly, transparent, comprehensible and accessible information on the data processing to both give and withhold consent where they have the capacity to understand the implications, and processing is in their own best interests, and in line with any age based laws in domestic and international legislation.

   c. Children should have the right to access appropriate, comprehensible, independent and effective complaints mechanisms and exercise their rights.

V. Recommendations for legislators and policy makers

- The use of digital technologies for educational purposes leads to the processing of personal data of children by a variety of actors (ranging from national governments, public and private educational settings, to private actors such as providers of products or services and software developers, as well as individuals such as teachers, legal guardians and peers). The data that is processed is not only provided by children, parents or educators, but also data that is created unconsciously or data that is inferred (for instance on the basis of profiling). Highly sensitive data, such as biometric data, are increasingly collected by educational institutions. Such data collection may have lifelong implications for children. Since situations arise when different authorities are under a legal obligation to co-operate a strict necessity and proportionality test should be applied before the collection of all personal data to ensure data minimisation and that any use will meet a child's reasonable expectations and meet the principles of purpose limitation, and restrictions regarding storage and retention. It is essential to acknowledge that it is not only the child's right to data protection that is affected when it comes to education and digital technologies and that the right to privacy and data protection are enabling rights to the protection of further rights and of the child. The right to non-discrimination, the right to development, the right to freedom of expression, the right to play and the right to protection from economic exploitation might also be at

stake. Legislators and policy makers should ensure that the full range of rights are ensured by other instruments, protocols, and guidelines where considering the implications of children's data processing in the context of education.

A. Review legislation, policies and practice

1. When applicable, e~~E~~nsure alignment with these principles and guidance, and promote their implementation in all data processing into, across and ~~out of~~after leaving the educational setting for the data life-cycle.

2. Set high expectations for privacy-by-design ~~standard~~ configurations, in standards for the technical requirements of procured services.

B. Offer effective support for children ~~'s~~ rights to be heard

2. Representation of child data subjects to supervisory authorities (Article 18) by third parties should be accessible and strengthened. States Parties may provide under Article 13 for extended protection in their legislation. It should be made possible that any body, organisation or association independently of a data subject's mandate, has the right to lodge a complaint with the competent supervisory authority, in that State Party, where permitted by Member State law, ~~and to exercise the rights referred to in the Convention~~ if it considers that the rights of a data subject have been infringed as a result of processing.

3. ~~M~~Establish procedures for children to express themselves and to make their voices heard in regard of exercising their right to privacy in educational settings and to ensure their view is taken into consideration.

4. Make it easy for a child to access remedies for violations of the provisions of the Convention under Article 12 and in the spirit of the Council of Europe Guidelines on child-friendly justice~~,~~ [20]providing the grounds for the necessary cooperation, and with mutual assistance between supervisory authorities (Articles 15, 16, and 17(3)) ~~and in the spirit of the Council of Europe Guidelines on child-friendly justice~~[21].

5. Remove any obstacles for children to get access to court, such as the cost of the proceedings or the lack of legal counsel in matters concerning data protection in an educational setting.

---

[20] Guidelines on child friendly justice adopted by the Committee of Ministers of the Council of Europe on 17 November 2010. See also Parliamentary Assembly Resolution 2010(2014) "Child-friendly juvenile justice: from rhetoric to reality", and the orientations on promoting and supporting the implementing of the Guidelines on child-friendly justice by the European Committee on Legal Co-operation (CDCJ(2014)15).

[21] ~~Guidelines on child friendly justice adopted by the Committee of Ministers of the Council of Europe on 17 November 2010. See also Parliamentary Assembly Resolution 2010(2014) "Child-friendly juvenile justice: from rhetoric to reality", and the orientations on promoting and supporting the implementing of the Guidelines on child-friendly justice by the European Committee on Legal Co-operation (CDCJ(2014)15).~~

~~(l)~~ Recognising that specific attention shall be given to the data protection rights of children and other vulnerable individuals, educational settings shall ensure that staff are trained to ensure adequate capability to understand their role in due diligence, and to be able to incorporate the right of the child to be heard in their exercise of the aims and purposes of the Convention and the activities set out in Article 2.

C. *Recognise and integrate the rights of the child ~~ensured by other instruments, protocols, and guidelines that have data protection implications~~*

1. Respect and fulfil the obligations and commitments within existing Council of Europe and United Nations standards on the rights of the child.[22] These Guidelines apply to all children, with a view to realising this right to education without discrimination, and on the basis of equal opportunity.

3. Respect the UN General comment No.16 (2013) on State obligations regarding the impact of the business sector on children's rights.[23] States must take steps to ensure that public procurement contracts are awarded to bidders that are committed to respecting children's rights, and states should not invest public finances and other resources in business activities that violate children's rights. States should take appropriate measures to prevent, monitor, and investigate violations by businesses in the educational setting and digital environment.

4. Recognise the obligations in Article 24 in the Convention on the Rights of Persons with Disabilities to education and with regard to inclusion and involvement in the decision making about adoption of technology, ensure universal accessibility by design, and promote equitable provision. ~~These Guidelines apply to all children, with a view to realising this right without discrimination, and on the basis of equal opportunity.~~

VI. Recommendations for data controllers

~~Recommendations on processing in practice for educational settings~~

There are many actors in the data processing chain who may be data controllers; not only educational institutions and government bodies, but providers of platforms, devices, programmes and applications. The latter commercial actors may also be data controllers in their own right, where they alone or jointly with others determine the nature of the processing as defined in Article 2 of the Convention 108+ and careful attention is needed to understand that the nature of the processing determines each role and not solely what is set out in contract terms. The obligations upon data controllers may not always fall solely on the educational setting as a result. To meet all the relevant data protection principles

[22] The UNCRC Article 29 1. States Parties agree that the education of the child shall be directed to: (a) The development of the child's personality, talents and mental and physical abilities to their fullest potential; (b) The development of respect for human rights and fundamental freedoms, and for the principles enshrined in the Charter of the United Nations. https://www.ohchr.org/en/professionalinterest/pages/crc.aspx and Principle 7 Declaration of the Rights of the Child (1959) (Proclaimed by the UN General Assembly, resolution 1386 (XIV), A/RES/14/1386, 20 November 1959)

[23] Committee on the Rights of the Child General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights https://www.unicef.org/csr/css/CRC_General_Comment_ENGLISH_26112013.pdf

For some children the use of adaptive technology can be an unwelcome signifier of their disability.

including data accuracy, necessity, and security; educational settings need to encourage a good data governance culture in which risk assessment proactively considers rights and freedoms as part of any processing or procurement process and data quality is proactively monitored and effectively managed through records management, supported by skills training, and policies.

1. Legitimacy and lawful basis

(a) According to paragraph 1 of Article 10 of Convention 108+, the obligation rests with the controller to ensure adequate data protection and to be able to demonstrate that data processing is in compliance with the applicable laws.

(b) ~~Stakeholders~~All parties involved in data processing in educational settings should clarify the responsibilities and accountability between roles ~~in educational settings~~ to establish legal authority and their duties as regards data processing, and when contracting with providers and third-party data processors.

(c) A child's special category of data, as defined in Article 6, requires enhanced protection when being processed, starting with the appropriate legal basis for the processing. Where there is no other lawful basis for processing, informed and freely given consent should be obtained from a legal guardian for the processing of health and other special categories of data, ~~and~~ recorded as an appropriate safeguard under Article 6(1) for a child, when processing is in the best interests of the child and~~. Such data~~ may be shared for purposes that go beyond their direct care and education, only with freely given, specific, informed and explicit consent of the data subject or their legal guardian.

(d) Consent can never be assumed, on behalf of legal guardians or children, to legitimise data processing by third party providers.

(e) Data controllers should recognise that children and legal guardians cannot give valid consent to the use of third-party data processors, where it cannot be freely refused and without detriment.

~~Contracts with commercial vendors to public education providers should prevent any changes of terms and conditions, where the change may affect the fundamental rights and freedoms of the data subject. Any such changes would by default, require a revision of the contract and notification to the data subject and their legal guardians.~~

~~Children should not be expected to enter into a contract with third parties, for example with an e-learning provider or application ordered by the educational setting. Personal data processing by such services, should be enabled with a legitimate basis laid down by law, and in a third-party agreement between the educational setting and the provider.~~

(f) The ~~validity~~powers of a~~the~~ legal guardian to exercise lawful rights including to consent on behalf of a child~~,~~ expires when the competent child reaches the age of lawful maturity as laid down in law in the Member State. The data subject (the child) should at request be informed of any ongoing data processing about them, to which the legal guardian gave consent, so as to be able to exercise the rights of the data subject, as an adult.

(g) Children should not be expected to enter into a contract with third parties, for example with an e-learning provider or application mandated by the educational setting. The educational setting should process children's data on the basis of a written contract between the setting and the third party. Personal data processing by such services should be carried out on a legitimate basis laid down by law.

(h) Contracts between third parties and education providers should prevent any changes of terms and conditions, that affect the fundamental rights and freedoms of the data subject. Any such changes would by default require a revision of the contract and notification to the data subject and their legal guardians explaining the proposed changes in a clear and straightforward way.

(i) To meet obligations to the rights of a child to education, settings should offer a suitable level of alternative provision of education without detriment to the child, should families or the child exercise the right to object to data processing in digital tools, as remedy in accordance with Article 9 (1)(f) of the Convention 108+.

(j) In line with Article 9(1)(d) ~~(d) the right to object to the processing of personal data concerning him or her,~~ advertising should not be considered legitimate grounds or a compatible purpose under Article 5(4)(b) that overrides a child's best interests, or their fundamental rights and freedoms~~undamental freedoms~~.[24]

(k) Data analytics and product development using personal data should not be considered legitimate compatible use~~grounds~~ for further processing that override a child's interests or rights and fundamental freedoms, or reasonable expectations of the data subjects in accordance with paragraph 49 of the Explanatory Report of the Convention.

(l) Controllers and processors ~~must~~shall not give away children's personal data ~~for others to monetise,~~ collected in the course of their education, for others to monetise, or reprocess it for the purposes of selling anonymised or de-identified data, for example to data brokers.

[24] The UNCRC Article 29 1. States Parties agree that the education of the child shall be directed to: (a) The development of the child's personality, talents and mental and physical abilities to their fullest potential; (b) The development of respect for human rights and fundamental freedoms, and for the principles enshrined in the Charter of the United Nations. https://www.ohchr.org/en/professionalinterest/pages/crc.aspx and Principle 7 Declaration of the Rights of the Child (1959) (Proclaimed by the UN General Assembly, resolution 1386 (XIV), A/RES/14/1386, 20 November 1959)

(m) Consistent with Member States' domestic law, codes of practice should set out ~~lawful practice~~guidance~~,~~ for situations where staff or children access educational software systems, databases or other third-party products through personal electronic devices or from home, and therefore mix personal data including metadata, from their private and family life~~,~~ with their professional or educational record.~~, in the use of third-party products, such as when accessing school software or databases from home.~~

2. Fairness

(a) ~~The principle of~~ Article 8(1)(e) of the Convention 108+ requires any data processing to be transparent, and complete and as set out in the Explanatory Report of the Convention 108+, that means in a way that can be fairly and effectively presented to a data subject, for example, according to the child's evolving capacity and in a child-friendly, comprehensible language and accessible alternative formats to text-only where ~~necessary~~appropriate in accordance with paragraph 68 of the Explanatory Report of the Convention. It should be interpreted in the educational context as necessary to be understood by a child according to their capacity, ~~or~~or by their legal guardians.

(b) Proactive provision of accessible information about the ~~child as data subject's~~ full range of data subject rights, available to the child and his or her legal guardian prior to the start of a data collection process, is necessary to meet transparency obligations. As a rule, both the child and legal guardians should ~~directly r~~receive the information directly. Provision of the information to the legal guardian should not be an alternative to communicating the information to the child, appropriate to their evolving capacity.

(c) Educational settings should carry out and publish at ~~setting~~institution level, a register of its data processing activities, a list of ~~p~~partners, such as vendors and subcontractors, data protection impact assessments, privacy notices and any amendments to terms and conditions over time.

(d) ~~They~~Educational settings should report ~~on breaches,~~ to Supervisory authorities as prescribed by Convention 108+ ~~if not~~ and to the data subjects themselves in the event of breaches and share audit reports to demonstrate their accountability and transparency of data processing with third-parties.

(e) Statements about personal data processed should be available on request, as part of s~~S~~ubject a~~A~~ccess rights. It may be recognised as good practice to offer such information through self-service tools, free to the child as data subject.

(f) Before transborder flows of personal data and subject to appropriate levels of protection according to Article 14 (3) and (4), the data subject and their legal guardians should be notified ~~and express their consent~~.

3. Risk assessment

(a) Controllers must assess the likely impact of intended data processing on the rights and fundamental freedoms of the child, prior to the commencement of data processing, and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms, with regard to Article 10(3) of the Convention 108+ and all its other principles.

~~Recognising that specific attention shall be given to the data protection rights of children and other vulnerable individuals, educational settings shall ensure that staff are trained to ensure adequate capability to understand their role in due diligence and the exercise of the aims and purposes of the Convention, and the activities set out in Article 2.~~

(g) The procurement of tools that process children's data~~,~~ shall ensure respect for ~~a~~ children as ~~the~~ data subjects and their legal guardian's rights and their reasonable expectations, as part of the decision-making ~~over~~in the introductions of any product~~;~~ whether bought~~,~~ or so-called freeware.

~~Measures should only be chosen if it can be demonstrated that the purpose of the processing could not be reasonably fulfilled by another means, which is less intrusive to the fundamental rights and freedoms of the data subject.~~

(h) Where freedom of information laws apply~~ies~~ to public bodies, Codes of Practice could include a suggestion as best practice that Data Protection Impact A~~a~~ssessments may be ~~used~~made accessible as part of routine publication schemes, to facilitate broad transparency and accountability.

(a) Children's voices should be heard in order to take their own perspective on risks in regard of their data being processed in due consideration.

4. Retention

(a) At the time when a child leaves education, only the minimum necessary amount of identifying data should be retained, and in the child's best interests, ~~such as~~in order to demonstrate attainment, safeguard their future rights of access, and to meet statutory obligations.

(c) Educational settings should not retain personal data in a form which permits identification for longer than necessary, and with due regard to the provisions of Article 5~~.~~(4), Article 7(2), Article 8~~.~~(1) and Article 9 of Convention 108+. Exceptions which respect the essence of the fundamental rights and freedoms of the child and constitute a proportionate measure, necessary in a democratic society for the purposes of Article 11 of Convention 108+, may apply.

(d) Upon leaving~~When a child leaves~~ each stage of compulsory education or when they change setting (across all ages, in nursery, primary, secondary, further and tertiary education) it should be best practice ~~they~~that children at request ~~that~~ should receive a full copy of their record including information about personal data retention and destruction, i.e. to be informed which personal data continue to be retained and processed, by whom, for what purposes, after the child has left the setting, and in any case the data controllers must maintain mechanisms that enable them to fulfil any ongoing obligations to the data subject.

(e) Because it is so difficult to de-identify data well, best practice ~~w~~should be to prohibit re-identification and require that third-parties do not attempt any re-identification, or allow others to do so after receipt of deidentified data. Recognise where it applies according to domestic law in some State Parties, that re-identification may be a criminal offence.

[New section] Securing personal data in an Education Setting

7.5.1 The protective measures applied to personal data should be based on a risk assessment following industry standards and best practice, and using established guidance such as ISO 17799:2000.

7.5.2 Applicable controls are likely to be a combination of authentication, authorisation and access control measures, and may be a combination of digital and non-digital measures.

7.5.3 The following factors should be considered:

- Physical accessibility (e.g. to devices and data in the education setting)
- Networked access to devices and data
- Backup and archival of data

7.5.4 Physical accessibility includes data collected or stored in at least the following contexts:

- classroom/e-learning (including distance learning outside school premises)
- school administration
- premises (physical access, CCTV including on school vehicles, biometric readers)

7.5.5 In the e-learning context, thought should be given to appropriate ways for children to authenticate to systems when authentication is required at all. Risk assessment should consider the method of authentication, balancing alternative approaches such as fully identifiable ID and password systems versus tokens and attribute-level authorisation. Assessment must be informed by the data protection principles of necessity, proportionality and data minimisation.

7.5.6 For networked access to data, authentication is almost certain to be required, and is desirable, to prevent unauthorised access. The same questions arise as for on-site access: what is the most appropriate authentication technology, and is access granted on the basis of individual identity (firstname.lastname) or an attribute ("pupil at this school").

7.5.7 Risk assessment prior to processing must also assess whether data is data protected against unauthorised access, modification and removal/destruction. Where data is processed off site (for example by third party service providers), education providers must remain aware of their ongoing responsibilities as data controllers. Due diligence must be done to establish the third party's ability to protect personal data appropriately, including confidentiality, integrity and availability.

7.5.8 Similar questions should be asked relating to digital data that is stored for backup and/or archival purposes, especially if these services are provided by third parties - either explicitly (such as for a contracted archival service) or implicitly,

as part of the data availability protections offered by an e-learning, administrative service.

7.5.9 Where encryption is not integrated into an application or service, it may be appropriate to encrypt data "manually" as stand-alone protective measure.

7.5.10 Numerous levels of protection can be applied (and even combined). Encrypted data should be managed in a similar way to backup/archive data. That is, the process of getting the data back again (from its encrypted state, or from its backup or archive) should be regularly tested. Consideration should be given to fallback procedures in case the person primarily responsible cannot perform this task.

B. ~~Recommendations on a~~Automated decisions and profiling

(a) Every individual has the right not to be subject to a decision significantly affecting them, based solely on an automated processing of data without having his or her views taken into consideration. Knowledge of the reasoning underlying the data processing where the results are applied to the data subject, should be made readily available, in accordance with Article 9(1)(a) and 9(1)(c) of Convention 108+.

(b) Profiling of children~~, which is any form of automated processing of personal data which consists of applying a "profile" to a child, particularly in order to take decisions concerning the child or to analyse or predict his or her personal preferences, behaviour and attitudes,~~ should ~~be~~ prohibited by law. In exceptional circumstances, States may lift this restriction when it is in the best interests of the child or if there is an overriding public interest, on the condition that appropriate safeguards are provided for by law (paragraph 37 of the Guidelines on the child in the digital environment).

(c) Children's attainment and achievement should not be routinely profiled in order to measure systems, for example, for measuring school or teacher performance management on the basis that this is not justified as an overriding ~~general~~public interest.

(d) The Guidelines on artificial intelligence and data protection[25] should be followed in educational settings, with regard to the automatic processing of personal data to ensure that AI applications do not undermine the human dignity, the human rights and fundamental freedoms of every child whether as an individual, or as communities, in particular with regard to the right to non-discrimination~~the right to data protection~~.

(e)

[25] Guidelines on Artificial Intelligence and Data Protection, document T-PD(2019)01, available at https://rm.coe.int/2018-lignes-directrices-sur-l-intelligence-artificielle-et-la-protecti/168098e1b7

A. Recognition of the rights of the child, as the data subject, and their legal guardians, are both necessary in an algorithmic decision-making context, associated with processing personal data using artificial intelligence and informed processing (see the Guidelines on data protection and artificial intelligence).[26]

(f) Data controllers have responsibility to carry out data protection and privacy impact assessments.~~,~~ These should have~~with~~ regard for the specific impact on children's rights ~~impact~~[27] and should demonstrate that the outcomes of algorithmic applications ~~used~~ are in the best interests of the child, and ensure that a child's development is not unduly influenced in opaque ways.

(g) Personalisation of content may (but does not always) constitute an intrinsic and expected element of certain online services, and therefore may be regarded as necessary for the performance of the contract in some cases between the service ~~buyer~~ supplier and the educational setting, but not in respect ~~with~~of the child since they cannot enter into a contract[28] even at the insistence of the educational setting.

(h) Predictions about groups or persons with shared characteristics based on ~~machine~~ analysis of large sets of personal data, ~~mus~~shall~~t~~ still be considered as processing personal data, even where there is no intention for it to result in an intervention with an individual.

(i) The distribution and use of software or use of services designed to observe and monitor user activity ~~use of~~on a terminal or communication network building a profile of behaviour~~,~~ should not be permitted, unless expressly provided for by domestic law, and accompanied by appropriate safeguards, as set out in Principle 3.8 of Council of Europe recommendation CM/Rec(2010)13 and explanatory ~~memorandum~~memorandum[29], on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

C. ~~Recommendations on b~~Biometric data

(a) Biometric data should not be routinely processed in educational settings. I~~and i~~n accordance with the principle of strict necessity, processing of such data should only be permissible in exceptional circumstances, after carrying out a data protection impact assessment, and where there is no less intrusive, alternative means of achieving the same aim.

26 Guidelines on Artificial Intelligence and Data Protection, document T-PD(2019)01, available at https://rm.coe.int/2018-lignes-directrices-sur-l-intelligence-artificielle-et-la-protecti/168098e1b7

[27] Committee on the Rights of the Child General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights paras 77-81 https://www.unicef.org/csr/css/CRC_General_Comment_ENGLISH_26112013.pdf

[28] Personalisation of content may (but does not always) constitute an intrinsic and expected element of certain online services, and therefore may be regarded as necessary for the performance of the contract with the service user in some cases. (EPDB, Guidelines 2/2019)

[29] Council of Europe recommendation CM/Rec(2010)13 and explanatory memorandum (2011) https://rm.coe.int/16807096c3

(b) Exceptions for use ~~in the~~to support c~~of people~~ hildren and educational staff with accessibility needs, for example on-screen eye tracking, for their direct benefit, and without discrimination[30], ~~may~~should be provided for ~~made with~~ with appropriate safeguards ~~and~~ enshrined in law.

(c) The use of biometrics in educational settings such as for identity verification including remote proctoring, shall only be allowed where no less invasive method may achieve the same aim, and with appropriate safeguards enshrined in law, in accordance with Article 6(1) of Convention 108+. This should include due regard for the risks that the processing of sensitive data may present for the rights and fundamental freedoms of the child, ~~notably~~including lifelong discrimination. Alternative methods should be offered without detriment.

~~Biometric data collected from children for the purposes of education, should remain within the educational setting and not be made available to third parties, for internal or external purposes of law enforcement, crime prevention, immigration or similar non-educational purposes, where it is not in the best interests of the child.~~

(d) Recognising that the definition of biometric data within Article 6 of the Convention is for uniquely identifying a person, authorities should also be alert to the sensitivities of processing bodily and behavioural data from a child, that may not be for verification of identity. The purposes of such data processing may be instead to influence the physical or mental experience of the child, such as in immersive virtual reality. ~~C~~Processing characteristics about voice, eye movement, and gait; social emotional and mental health, and mood; and reactions to neurostimulation, for the purposes of influencing or monitoring a child's behaviour should ~~be considered~~ be done on the basis of a precautionary principle and treated as biometric data are under the Convention 108+~~. Personal data about a child's physical or emotional development should be processed with extreme caution and sensitivity,~~ , even when it is not for the purposes of uniquely identifying the person.

(e) Educational settings should pay particular attention to where their use of a service constitutes a contractual agreement, for example in the use of videoconferencing software in order to be able to implement distant learning programs, and in which staff may agree to terms-and-conditions of service that include the processing and recording of content including children's images and voice data. Staff should ensure that where data processing is on the basis of consent, that consent cannot be assumed by the education setting and granted on behalf of the child, but must be freely given by the data subject, the child in accordance with their evolving capacities or their legal guardian.

[30] For some children the use of adaptive technology can be an unwelcome signifier of their disability. Two clicks forward and one click back: Report on children with disabilities in the digital environment. The Council of Europe (2019) https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f

VII. Recommendations for industry cooperation

Supervisory authorities ~~should~~ may develop these guidelines into Codes of Practice on the basis of a wide cooperation with developers and industry, with education practitioners, academia, with organisations representing teachers and families, and civil society and with children themselves. Standards may include minimum criteria or clear guidelines for procurement in relation to products or services in relation to children's data processing, including products or services offered for free or at a low cost, and in any product and research trials.

1. Standards

(a) Since children merit special protection, the expected standards for the processing of children's data in the education sector should set a high bar by design, to meet appropriate standards of quality and the rule of law, and data protection by design and by default.

(b) Standards may be set out in Codes of Practice and certification which should be drafted on the basis of a wide cooperation with developers and industry, with education practitioners, academia, with organisations representing teachers and families, and civil society and with children themselves.

(c) Provisions of lawful data processing contracts, agreed at the time of the procurement should also continue to apply after the purchase, merger, or other acquisition by another entity. There must be a sufficiently fair communication period of any change of terms and the right to alter or object to new conditions, end the contract and withdraw student data on request.

~~A contractual requirement on providers to give notice of changes to terms of service is good, but agreement not to change terms and conditions without consent is better.~~

2. Transparency

(b) Developers must ensure that their own understanding of all the functionality of products they design~~,~~ can be sufficiently explained to meet regulatory and lawful requirements, and avoid creating a high investigative burden by design, inappropriate for staff in educational settings and children.

(d) Privacy information and other published terms and conditions, policies and community standards, must be concise, and written in clear language appropriate for children. Child-friendly communication methods need not dilute the explanations that are necessary for fair processing, but should not be excessive, and should be separate from legal and contractual terms for legal guardians and educators. Layered privacy notices could help to combine the need of a complete but at the same time efficient information.

3. Design features with data protection and privacy implications

(a) Expectations of respect for the principles of data protection by design and default should ~~include~~prevent ~~using~~ design that ~~does not~~ include~~s~~ features that may encourage children to provide unnecessary personal data or to lower their privacy settings.

(b) Processing personal data for the purposes of service improvement and security must be ~~narrow~~strictly necessary and within the confines of the delivery of the core service as well as the reasonable expectations and delivery of the contracted service to users~~, such as security enhancement~~.

(c) Data analytics[31] based on personal data and user tracking should not be considered a form of service improvement or security enhancement and not be necessary for performance of a contract.

(d) Product enhancements, for example those intended to add new features to an application or improve its performance, ~~s~~should require new acceptance or consent, and opt-in before installation. Where another lawful basis is relied upon other than contract, the data subject must be informed ahead of the upgrades, and in accordance with the lawful basis.

(e) ~~Additional weight should be given to Article 14 under the Convention~~Specific attention should be given to Article 14 under the Convention, to make sure transborder flows of personal data for the purposes of education meet the conditions of the article, to limit transborder flows of personal data for the purposes of education, and to ensure that transborder flows take place within a recognised data protection framework and within domestic law.

(f) Geolocation tracking in order to identify the location of use, the user, to target in-~~-~~app functionality, or for profiling purposes, ~~which~~ should be deployed~~provided~~ only when necessary and according to an appropriate legal basis. Services ~~,~~ should provide an indicator when the location tracking is active and allow ~~an~~ easy disabling without loss of essential functionalities. Such profiles and history should be easy to delete at the close of a session.

(g) ~~Processing data in~~ Children's data collected by means of educational software tools~~,~~ should not ~~not be permitted~~be processed to serve or target behavioural advertisements, for real time bidding advertising technology, or for in-~~-~~app advertising, to serve children or families marketing, for product upgrades or additional vendor driven products.

[31] Guidelines on the protection of individuals on the processing of person data in a world of Big Data (2017) T-PD(2017)01

1. Introduction

Much commercial software in education is known as 'freeware'; software offered to educational settings at no direct financial cost. According to the EU e-commerce Directive (Art 1.1) this would generally fall within the definition of an Information Society Service[4] "provided for remuneration", where the personal data processed about the user in exchange for the service must be understood as a kind of remuneration.

These guidelines should also apply wherever remote e-learning solutions are engaged as the result of a child's enrolment at an educational setting and are used outside the educational setting such as for homework or distance learning. Distance learning tools and resources should be subject to the same rigorous due diligence for pedagogical quality, safety and data protection standards, for instance regarding the default settings, so that the usage of applications and software does not infringe the rights of the data subjects (data protection by default). Processing must not involve more data than necessary to achieve the legitimate purpose. This is particularly important when consent is not possible to be freely given, when the choice is to use a product and receive remote instruction, or not and receive none.

When a school requires the use of e-learning tools, a consent basis for processing personal data either by the school or by the third-party processor will not be valid, because consent must be unambiguously freely given and able to be refused without detriment.[7][32]

4. Principles of data processing

4.6. Assessment of the likely impact of the intended processing on the rights and freedoms of the data subject prior to the commencement at the start of any data processing and across its life cycle. Particular attention needs paid at an early stage, as to how communication about data processing will be maintained, between the data controller and the child or their legal guardian, after the child has left the educational setting.

4.8. Specific to the educational context, data controllers must recognise the rights of legal guardians to act on behalf of and in their child's best interests in accordance with domestic and international law. Best effort should be made to involve a child in decisions

[32] In this context, it should also be taken into account that recital 43 of the GDPR states that "in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is *a clear imbalance between the data subject and the controller*, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation" and that children in an educational setting constitute a typical example of a situation where there is an imbalance between the data subject and the controller and where another legal basis should rather be applied

about them and provide suitable information to families, where appropriate.

6. Recommendations for legislators and policy makers

The use of digital technologies for educational purposes leads to the processing of personal data of children by a variety of actors (ranging from national governments, public and private educational settings, to private actors such as providers of products or services and software developers, as well as individuals such as teachers, legal guardians and peers). The data that is processed is not only provided by children, parents or educators, but also data that is created unconsciously or data that is inferred (for instance on the basis of profiling). Highly sensitive data, such as biometric data, are increasingly collected by educational institutions. Such data collection may have lifelong implications for children. (…)

6.3. Offer effective support for children's rights to be heard

6.3.1. Provide Supervisory Authorities with sufficient resources to ensure that data protection laws are adequately applied in the educational setting and related technologies used consistently.

6.3.2. Representation of child data subjects to supervisory authorities (Article 18) by third parties should be accessible and strengthened. States Parties may provide under Article 13 for extended protection in their legislation. It should be made possible that any body, organisation or association independently of a data subject's mandate, has the right to lodge a complaint with the competent supervisory authority, in that State Party, where permitted by Member State law, if it considers that the rights of a data subject have been infringed as a result of processing.

6.3.3. Establish procedures for children to express themselves and to make their voices heard in regard of exercising their right to privacy in educational settings and to ensure their view is taken into consideration.

6.3.4. ~~Make it easy for a child to access~~ remedies for violations of the provisions of the Convention under Article 12 and in the spirit of the Council of Europe Guidelines on child-friendly justice[15] providing the grounds for the necessary cooperation, and with mutual assistance between supervisory authorities (Articles 15, 16, and 17(3)).

6.3.6. Recognising that specific attention shall be given to the data protection rights of children and other vulnerable individuals, educational settings shall ensure that staff are trained to ensure adequate capability to understand their role in due diligence, and to be able to incorporate the right of the child to be heard in their exercise of the aims and purposes of the Convention and the activities set out in Article 2.

7. Recommendations for data controllers

There are many actors in the data processing chain who may be data controllers; not only educational institutions and government bodies, but providers of platforms, devices, programmes and applications. The latter commercial actors may also be data controllers in their own right, where they alone or jointly with others determine the nature of the processing as defined in Article 2 of the Convention 108+ and careful attention is needed to understand that the nature of the processing determines each role and not solely what is set out in contract terms. The obligations upon data controllers may not always fall solely on the educational setting as a result. To meet all the relevant data protection principles including data accuracy, necessity, and security; educational settings need to encourage a good data governance culture in which risk assessment proactively considers rights and freedoms as part of any processing or procurement process and data quality is proactively monitored and effectively managed through records management, supported by skills training, and policies.

7.1. Legitimacy and lawful basis

7.1.6. The powers of a legal guardian to exercise lawful rights including to consent on behalf of a child expires when the competent child reaches the age of lawful maturity as laid down in law in the Member State. The data subject (the child) should be informed of any ongoing data processing about them, to which the legal guardian gave consent, so as to be able to exercise the rights of the data subject, as an adult.

7.1.8. Contracts between third parties and education providers should prevent any changes of terms and conditions, that affect the fundamental rights and freedoms of the data subject. Any such changes would by default require a revision of the contract and notification to the data subject and their legal guardians explaining the proposed changes in a clear and straightforward way.

7.1.10. In line with Article 9(1)(d) advertising should not be considered legitimate grounds or a compatible purpose under Article 5(4)(b) that overrides a child's best interests, or their fundamental rights and freedoms.

7.1.11. Data analytics and product development using personal data should not be considered legitimate compatible use for further processing that override a child's interests or rights and fundamental freedoms, or reasonable expectations of the data subjects in accordance with paragraph 49 of the Explanatory Report of the Convention.

7.2. Fairness

7.2.6. Before transborder flows of personal data and subject to appropriate levels of protection according to Article 14 (3) and (4), the data subject and their legal guardians should be notified.

7.3.4. Children's voices should be heard in order to take their own perspective on risks in regard of their data being processed in due consideration.

7.4. Retention

7.4.4. Upon leaving each stage of compulsory education or when they change setting (across all ages, in nursery, primary, secondary, further and tertiary education) it should be best practice children that should receive a full copy of their record including information about personal data retention and destruction, i.e. to be informed which personal data continue to be retained and processed, by whom, for what purposes, after the child has left the setting, and in any case the data controllers must maintain mechanisms that enable them to fulfil any ongoing obligations to the data subject.

7.5. Securing personal data in an Education Setting

7.5.1. The protective measures applied to personal data should be based on a risk assessment following industry standards and best practice, and using established guidance (such as ISO 17799:2000).

7.5.2. Applicable controls are likely to be a combination of authentication, authorisation and access control measures, and may be a combination of digital and non-digital measures.

7.5.3. The following factors should be considered:

- Physical accessibility (e.g. to devices and data in the education setting)
- Networked access to devices and data
- Backup and archival of data

7.5.5. In the e-learning context, thought should be given to appropriate ways for children to authenticate to systems when authentication is required at all. Risk assessment should consider the method of authentication, balancing alternative approaches such as fully identifiable ID and password systems versus tokens and attribute-level authorisation. Assessment must be informed by the data protection principles of necessity, proportionality and data minimisation.

7.5.6. For networked access to data, authentication is almost certain to be required, and is desirable, to prevent unauthorised access. The same questions arise as for on-site access: what is the most appropriate authentication technology, and is access granted on the basis of individual identity (firstname.lastname) or an attribute (“pupil at this school”).

7.5.9. Where encryption is not integrated into an application or service, it may be appropriate to encrypt data “manually” as stand-alone protective measure.

7.5.10. Numerous levels of protection can be applied (and even combined). Encrypted data should be managed in a similar way to backup/archive data. That is, the process of getting the data back again (from its encrypted state, or from its backup or archive) should be regularly tested. Consideration should be given to fallback procedures in case the person primarily responsible cannot perform this task.

7.6. Automated decisions and profiling

7.6.7. Personalisation of content may (but does not always) constitute an intrinsic and expected element of certain online services, and therefore may be regarded as necessary for the performance of the contract in some cases between the service supplier and the educational setting, but not in respect of the child since they cannot enter into a contract[22] even at the insistence of the educational setting.

7.6.9. The distribution and use of software or use of services designed to observe and monitor user activity on a terminal or communication network building a profile of behaviour should not be permitted, unless expressly provided for by domestic law, and accompanied by appropriate safeguards, as set out in Principle 3.8 of Council of Europe recommendation CM/Rec(2010)13 and explanatory memorandum [23] , on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

8. Recommendations for industry cooperation

Supervisory authorities should develop these Guidelines into Codes of Practice on the basis of a wide cooperation with developers and industry, with education practitioners, academia, with organisations representing teachers and families, and civil society and with children themselves. Standards may include minimum criteria or clear guidelines for procurement in relation to products or services in relation to children's data processing, including products or services offered for free or at a low cost, and in any product and research trials.

8.3.7. Children’s data collected by means of educational software tools should not be processed to serve or target behavioural advertisements, for real time bidding advertising technology, or for in-app advertising, to serve children or families marketing, for product upgrades or additional vendor driven products.