COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

12 June 2020

T-PD(2019)06BISrev3

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

## CONVENTION 108

## Children's Data Protection in an Education setting

## Draft Guidelines

Directorate General of Human Rights and Rule of Law

# Contents

The digital environment shapes children's lives in many ways, creating opportunities and risks to their well-being and enjoyment of human rights. Some digital tools enable the delivery of essential information, connecting school communities outside the classroom. Others provide ways to sharing educational content or offer vital alternative means and modes of education through assistive technology and augmented communications.

These guidelines[1] should support organisations and individuals in the context of education to respect, protect and fulfil the data protection rights of the child in the digital environment, within the scope of Article 3 of the modernised Convention 108 (more commonly referred to as "Convention 108+")[2], and in accordance with the CoE instruments including the Guidelines on Children in the Digital Environment Recommendation CM/Rec(2018)7[3].

The UN Convention Committee on the Rights of the Child set out in 2001, that

> *"Children do not lose their human rights by virtue of passing through the school gates. Education must be provided in a way that respects the inherent dignity of the child and enables the child to express his or her views freely..."*

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.

Much commercial software in education is' freeware', software offered to educational settings at no cost, often in a non-explicit exchange for personal data. The expansion of educational technology means non-state actors routinely control children's educational records.

The digital infrastructure to deliver state education is often commercially owned. This can introduce new questions of where control of the curriculum sits, and questions of security and sustainability. Companies can lock in proprietary software practices, with consequences for interoperability, for data access and reuse, and the budgetary and environmental impacts of obsolescence. It is common, at the time of writing, for small companies to be incubated by angel investors and later be bought out by larger companies. Control of personal data can 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 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 alone.



[1] The Guidelines follow and build on the report "Children's Data Protection in Education Systems: Challenges and Possible Remedies" drafted by Jen Persson, Director of defenddigitalme, available at https://rm.coe.int/t-pd-2019-06rev-eng-report-children-data-protection-in-educational-sys/168098d309

[2] Convention 108+: Convention for the protection of individuals with regard to the processing of personal data as modernised by the Amending Protocol CETS 223, available at: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 .

[3] Council of Europe Guidelines on Children in the Digital Environment Recommendation CM/Rec(2018)7 https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

The investigative burden in educational settings can make it hard even for adults to understand software tools and their processing, to carry out adequate risk assessment, to retrieve and offer the relevant information required to provide to the data subjects, and be able to meet and uphold users 'rights, including the comparative implications of using open or proprietary ICT, paid-services or freeware.

Educational 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 education, creating a fair playing field for everyone.

Stakeholders, including legislators and policy makers, educational authorities and industry, should follow 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 in educational settings, where children are recognised as vulnerable due to their lack of understanding and capacity, disempowerment, and state of being in the process of development into adulthood.

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."*[4]

These guidelines should also apply wherever remote e-learning solutions are used outside the educational setting. 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. It 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, any consent required by companies must be freely given 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.

[4] Working Paper in English: Working Paper on E-Learning Platforms (Washington D.C. (USA), 24./25. April 2017) https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/

Today's adults should ensure that protections offered to children are not only appropriate for the duration of their childhood, but also consider their 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 human flourishing.

## I. Scope and Purpose

1. These Guidelines seek to help explain the data protection principles of "Convention 108+" to tackle the challenges in the protection of personal data brought by new technologies and practices, whilst maintaining technologically neutral provisions.

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 is the right 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.

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[5]. These Guidelines also take into account the new safeguards of Convention 108+.

## II. Definitions for the purposes of the Guidelines

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

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

(c) "direct care and education" means a learning, administrative or social care activity concerned with the direct delivery of teaching and its administration, or the immediate care of an identified individual, generally falling within the statutory public tasks of education and the data processing for which, the child and legal guardians would reasonably expect as part of being in school. Direct care is contrasted with Secondary Re-uses of data, which are all other indirect uses of personal data collected or inferred about an individual in the context of their time spent 'in loco parentis' with an educational setting; non-exhaustive examples include learning analytics, risk prediction, public interest research, for processing by in the press or social media, and marketing purposes;

(d) "educational setting" means an environment for the delivery of education to a child, subject to the jurisdiction of States Parties in the private and public sectors, but not by an individual in the course of purely household activities;

[5] 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

(e) "e-learning" may broadly include learning with the support of information and communication technologies (ICT), especially for delivery or accessing of content, distance learning or web-based learning (including tools used in online and offline modes). e-learning can take place without any live connection to a network or Internet connectivity but will often require such access as part of the service.

(f) "legal guardians" refers to the persons who are considered to be the parents of the child according to national law and have parental responsibilities; 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.

(g) "learning analytics" can be described as the measurement, collection, analysis and reporting of data about learners and their contexts, for purposes of understanding and optimising learning and the environments in which it occurs.[6]

(h) "processing" means any operation or set of operations performed on personal data, such as 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;

(i) "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;

(j) "special category of data" has the same meaning as Article 6 of Convention 108+;

(k) "Supervisory Authorities" means authorities designated as be responsible for ensuring compliance with the provisions of Chapter IV of Convention 108+.

## 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 in an educational setting:

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

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

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

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

4. The accountability of data controllers and data processors, to 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. An assessment of the likely impact of the intended processing at the start of any data processing and across its life cycle.

7. 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)[7] .

8. Security measures[8] 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.

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

1. The Guidelines build on the existing principles enshrined in Convention 108+, the Council of Europe Strategy for the Rights of the Child (2016-2021)[9] and the case law of the European Court of Human Rights.

2. Every child is entitled to enjoy the full range of human rights safe-guarded by the European Convention on Human Rights, the United Nations Convention on the Rights of the Child (UNCRC) and other international human rights instruments.

3. These Guidelines encourage States Parties to Convention 108 to recognise these rights in the context of children's data protection in education.

### A. The best interests of the child

1. The best interests of the child shall be a primary consideration in all actions concerning the child in the digital environment.

[7] 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

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

[9] The Council of Europe Strategy for the Rights of the Child (2016-2021) https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168066cff8

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

3. Specific considerations may need to be given to the definition of best interests to more vulnerable children in education, such as those without parents, migrant children, refugee and asylum-seeking children, unaccompanied children, children with disabilities, homeless children, Roma children, and children in residential, medical or young offender institutions.

## B. The capacity of a child

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

2. As set out in the Guidelines to respect, protect and fulfil the rights of the child in the digital environment[10], all stakeholders should recognise the evolving capacities of children, including those of children with disabilities or in vulnerable situations, and ensure that policies and practices are adopted to respond to their respective needs in relation to the digital environment.

## **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 children are aware of their rights in the digital environment specifically as regards the education system and implement measures to ensure that they are able to access mechanisms for enforcing their rights.

2. Stakeholders should establish a default position of involving legal guardians in decisions before processing their children's personal data, to ensure personal data shall be processed fairly and in a transparent manner aligned with Article 5(4)(a); unless sharing such information poses a risk to the child's best interest.

3. In accordance with States Parties' law, 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.

[10] Council of Europe Guidelines on Children in the Digital Environment Recommendation CM/Rec(2018)7 https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

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

a. Children should be enabled to both give and withhold consent where they have the capacity to understand the implications, and processing is in their own best interests.

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

## V. Recommendations for legislators and policy makers

### A. Review legislation, policies and practice

1. Ensure alignment with these principles and guidance, and promote their implementation in all data processing into, across and out of the educational setting.

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

3. Maintain or establish a framework, including independent mechanisms as appropriate, to promote and monitor the implementation of these guidelines, in accordance with their educational, supervisory and administrative systems.

### B. Offer effective support for children’s rights to be heard

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.

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, 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. Make it easy for a child to access remedies for violations of the provisions of the Convention under Article 12, 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[11].

4. Remove any obstacles for children to get access to court, such as the cost of the proceedings or the lack of legal counsel.

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

1. Respect, protect and fulfil the rights of the child in the digital environment, in an educational setting, in accordance with the Guidelines on Children in the Digital Environment[12].

2. Respect the UN General comment No.16 (2013) on State obligations regarding the impact of the business sector on children's rights.[13] 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.

3. Recognise the obligations in Article 24 in the Convention on the Rights of Persons with Disabilities to education. 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

### A. Recommendations on processing in practice for educational settings

#### 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 law.



[11] 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).
[12] Council of Europe Guidelines on Children in the Digital Environment Recommendation CM/Rec(2018)7 https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a
[13] 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.

(b) Stakeholders 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, require 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.

(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 cannot give valid consent to the use of third-party data processors, where it cannot be freely refused without detriment.

(f) 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.

(g) 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.

(h) The validity of the legal guardian to exercise lawful rights 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 should be informed of any ongoing data processing to which the legal guardian gave consent, so as to be able to exercise the rights of the data subject, as an adult.

(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) the right to object to the processing of personal data concerning him or her, advertising should not be considered a compatible purpose under Article 5(4)(b) that overrides a child's best interests, or their rights and fundamental freedoms.[14]

[14] 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.

(k) Data analytics and product development using personal data should not be considered legitimate grounds for processing that override a child's interests or rights and fundamental freedoms.

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

(m) Consistent with Member States' domestic law, codes of practice should set out lawful practice, for situations where staff or children access educational software systems through personal electronic devices, and therefore mix personal data 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 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, in a child-friendly language where necessary. It should be interpreted in the educational context as necessary to be understood by a child according to their capacity, or their legal guardians.

(b) Proactive provision of accessible information about the child as data subject's full range of rights, 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 receive the information. Provision of the information to the legal guardian should not be an alternative to communicating the information to the child, appropriate to their capacity.

(c) Educational settings should carry out and publish at setting level, a register of its data processing partners, such as vendors and subcontractors, data protection impact assessments, privacy notices and any amendments to terms and conditions over time. They should report on breaches, to Supervisory authorities as prescribed by Convention 108+ if not to the data subjects themselves and share audit reports to demonstrate their accountability and transparency of data processing with third-parties.

(d) Statements about personal data processed should be available on request, as part of Subject Access rights. It may be recognised as good practice to offer such information through self-service tools, free to the child as data subject.

(e) 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 and all its other principles.

(b) 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.

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

(d) 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.

(e) Where freedom of information law applies to public bodies, Codes of Practice could include a suggestion that Data Protection Impact assessments may be used as part of routine publication schemes, to facilitate broad transparency and accountability.

## 4. Retention

(a) At the time when a child leaves education, the minimum necessary amount of identifying data should be retained, and in the child's best interests, such as to demonstrate attainment, safeguard their future rights of access, and to meet statutory obligations. Personal data that leave an educational setting should not be preserved in a form that permits identification for any longer than necessary, in accordance with Article 5 (4)(e).

(b) 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. 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, may apply.

(c) 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) they 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.

(d) Because it is so difficult to de-identify data well, best practice would 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.

## B. Recommendations on 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, should be made readily available, in accordance with Article 9(a) and 9(c).

(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 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 interest.

(d) The Guidelines on artificial intelligence and data protection[15] 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 individual, in particular with regard to the right to data protection.

(e) Data protection and privacy impact assessments, with regard for specific child rights impact[16] should demonstrate that algorithmic applications are in the best interests of the child, and that a child's development is not unduly influenced in opaque ways.

(f) 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 and the educational setting, but not with the child since they cannot enter into a contract[17] at the insistence of the educational setting.

[15] 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

[16] 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

[17] 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)

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

(h) The distribution and use of software designed to observe and monitor use of 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[18], on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

## C. Recommendations on biometric data

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

(b) Exceptions for use in the support of people with accessibility needs, for example on-screen eye tracking, for their direct benefit, and without discrimination19, may be made 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). 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 lifelong discrimination.

(d) 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.



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

19 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

(e) 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. 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 as biometric data. 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.

## VII. Recommendations for industry

### A. 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 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.

(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.

### B. Transparency

(a) 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 educational settings and children.

(b) 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 notice could help to combine the need of a complete but at the same time efficient information.

### C. Design features with data protection and privacy implications

(a) Expectations of respect for the principles of data protection by design and default should include using design that does not include 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 must be narrow 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 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. Product enhancements, for example those intended to add new features to an application or improve its performance, should require new acceptance or consent, and opt-in before installation.

(d) Additional weight should be given to Article 14 under the Convention, 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.

(e) Geolocation tracking in order to identify the location of use, the user, to target in app functionality, or for profiling purposes, which should be provided only when necessary and according to appropriate legal basis, should provide an indicator when the location tracking is active and allow an easy disabling. Such profiles and history should be easy to delete at the close of a session.

(f) Processing data in educational software tools, should not be permitted 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.