COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

11 February 2020 T-PD(2020)06BISRev2

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 Education Systems

Draft Guidelines

by Jen Persson, Director of defenddigitalme

Directorate General of Human Rights and Rule of Law

The opinions expressed in this work are the responsibility of the author and do not necessarily reflect the official policy of the Council of Europe

The digital environment shapes children's lives in many ways, creating opportunities and risks to their well-being and enjoyment of human rights. With the present Guidelines, the Consultative Committee of Convention 108 aims at addressing specifically the protection of personal data in education systems, preventing possible adverse consequences for children and enabling respect of their rights to privacy and data protection (Article 8 of the European Convention on Human Rights).

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..."*

For a variety of motivations, there is a rapid growth of commercial actors and emerging technologies in the global education technology (edTech) market across the world. The implications of the introduction of externally controlled digital tools to the classroom, and the wide range and volume of actors that process children's personal data often outside their country of residence, must not be underestimated.

Many commercial software in education are 'freeware', software offered to schools at no cost, often in a non-explicit exchange for personal data. The rapid expansion of educational technology has meant thousands of companies control millions of children's school records. Small companies may be incubated by angel investors and are later bought out by larger companies. Ownership can be transferred in takeovers multiple times in the course of a child's education. The child and family may never know. Companies often require schools to accept edits to standard terms and conditions, or face losing core software at no notice.

Under economic pressures to deliver low-cost state education, and marketisation, the infrastructure used to deliver state education may be commercially owned. This can introduce new risks and questions of security and sustainability, and can lock in proprietary software practices, with consequences for interoperability, for data access and reuse, and the budgetary and environmental impacts of obsolescence.

Children cannot see or understand how large their digital footprint has become or how far it is distributed 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 consensus that children cannot, and should not, be expected to understand a very complex online environment alone.

The investigative burden in schools can be too great even for teaching staff to be able to understand software tools and their processing, to carry out adequate risk assessment, retrieve and offer the relevant information required to provide to the data subjects, and be able to meet and uphold users' rights. School staff often accept data processing by vendors. without understanding their full product functionality or implications for children's data rights.

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.

Children's reputation is protected under Article 16 of the Convention of the Rights of the Child. It is important that the integrity and agency of future generations should be assured by providing children with a childhood where they can grow and learn untouched by unsolicited monitoring, profiling, habitualisation, and manipulation for companies' future purposes.
It is furthermore for today's adults to ensure that protections offered to children are not only appropriate for the duration of their childhood, but also consider the interests of the future adult, and promote the ability of children to reach adulthood unimpeded, and able to develop fully and freely, to meet their full potential and human flourishing. Good practice, free from exploitation, will enable a trustworthy environment fit for the future, so families can send their children safely to school, without future impediment as a result.

Legislators and policy makers, educational authorities and staff, unions, developers, manufacturers and vendors, children's representatives and civil society, should raise awareness of, translate and promote the use of these Guidelines in meeting data protection and privacy obligations within the scope of Article 3 of Convention 108, as well as make them available to children and their representatives, in a child-friendly and accessible manner.

Stakeholders should collaborate to create a rights-respecting environment, to uphold the human dignity, rights and fundamental freedoms of every individual, in respect of data protection, and in particular to support the rights of the child.

Policy makers have obligations to respect, protect and fulfil the rights of the child in the digital environment, in accordance with the CoE Guidelines on Children in the Digital Environment Recommendation CM/Rec(2018)7[1].

Nothing in the Guidelines shall be interpreted as precluding or limiting the provisions of the European Convention on Human Rights and of Convention 108. These Guidelines also take into account the new safeguards of the modernised Convention 108 (more commonly referred to as "Convention 108+").

1. Summary of recommendations for policy makers and education authorities

1.1 Recommendations on legitimate processing in practice

a. Review legislation, policies and practice to ensure alignment with these recommendations, principles and further guidance, promote their implementation in all data processing into, across and out of the education sector. According to paragraph 1, the obligation on the controller to ensure adequate data protection is linked to the

[1] 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

responsibility to verify and be in a position to demonstrate that data processing is in compliance with the applicable law. The data protection principles set out in the Convention, which are to be applied at all stages of processing, including the design phase, aim at protecting data subjects and are also a mechanism for enhancing their trust.

b. To uphold Article 1 and the purpose of the Convention, education authorities must clearly assign roles, responsibilities and accountability between school staff and other relevant persons to establish legal authority and their duties in data processing, and when dealing and contracting with providers and third-party data processors. A possible measure that could be taken by the controller to facilitate such a verification and demonstration of compliance would be the designation of a "data protection officer" entrusted with the means necessary to fulfil his or her mandate. Such a data protection officer, whose designation should be notified to the supervisory authority, could be internal or external to the controller in a school or educational authority.

c. Supervisory authorities should ensure high standards of privacy, security architecture including encryption, and data protection laws are applied to educational technology consistently and enforced in cooperation and with mutual assistance.

d. Controllers and processors should choose privacy-friendly standard configurations, when setting up the technical requirements for default settings, so that the usage of applications and software does not infringe the rights of the data subjects (data protection by default), notably to avoid processing more data than necessary to achieve the legitimate purpose.

e. Data shall be by default minimised, adequate, relevant and not excessive in relation to the purposes for which they are processed, not only at the point of collection, but throughout the data life cycle. Controllers and, where applicable, processors, must examine 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 of the Convention.

f. Personal data processing that may reveal or infer racial or ethnic origin, political opinions, trade union membership, religious or other beliefs, health or sexual life, behavioural data as relate to offences, criminal proceedings and convictions, in the context of educational records, must be recognised as special categories of data, under Article 6. Furthermore, where processing of a child's image is intended to reveal racial, ethnic or health information, such processing will be considered as processing of sensitive data. In order to prevent adverse effects for the child, processing needs to be accompanied by appropriate safeguards, adapted to the risks at stake, and the interests rights and freedoms to be protected.

g. The legitimacy of data processing under Article 5 of the Convention, for explicit, specified and legitimate purposes, by educational authorities, should not be compromised by excessive processing by contracted third-parties. Schools should be

determining the purposes of processing most often as necessary and proportionate in their public task and asking third parties to help them carry it out. In general, schools should be considered as data controllers, and third parties generally be processors, with joint controllership as exceptional rather than routine.

h. Contracts with commercial vendors to public education providers should prevent any significant changes of terms and conditions, where the change may affect the fundamental rights and freedoms of the data subject, without informing schools, children, and legal guardians. Authorities should offer the opportunity to cease processing with regard to Article 9 of the Convention, in a suitably appropriate timeframe.

i. Children cannot enter into a contract with third parties, for example with e-learning providers. Appropriate processing by such services, must be able to be provided through a school on a legitimate basis laid down by law, within users' reasonable expectations, and without detriment for those who object to such systems.

j. Written records of informed and freely given consent to opt-in to data sharing should be obtained from a legal guardian for the processing of health and other special category data, as an appropriate safeguard under Article 6(1) for a child, where there are no other legitimate basis for processing, and where appropriate safeguards are enshrined in law, in the best interests of the child.

k. Data re-use for the non-educational purposes of the child, beyond their own care or best interests, such as the distribution of personal data to any employer, charity, to the media, or for research purposes, should only be with the express and freely given consent of the legal guardian, child, or data subject. Restrictions on the exercise of these provisions may be provided for by law with respect to Article 11(2) and (3) .

l. 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).

1.2 Recommendations for representation and redress of children's rights

a. The best interests of the child shall be a primary consideration in all actions concerning the child in the digital environment, including the education sector. In assessing the best interests of a child, States should make every effort to balance, and wherever possible, reconcile a child's right to protection with other rights, in particular the right to freedom of expression and information, the right to be heard, as well as privacy and participation rights.

b. The capacities of a child develop from birth to the age of 18. As set out in, Recommendation CM/Rec (2018)7 of the Committee of Ministers and Guidelines to respect, protect and fulfil the rights of the child in the digital environment, *"Individual children reach different levels of maturity at different ages. States and other relevant 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. This also means, for example, that policies adopted to fulfil the rights of adolescents may differ significantly from those adopted for younger children."

c. 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 and other controllers should ensure that children are made aware of how to exercise all of their rights to privacy and data protection in accordance with Article 9, taking into account their age and maturity and, where appropriate, with the direction and guidance of their legal guardians or other persons legally responsible for the child in a manner consistent with the evolving capacities of the child, in the school environment. Further support should be offered if it comes to seeking redress.

d. Information to be provided about or to a data subject in education, must be tailored to a child, in a proactive manner. Subject Access Request processes must be understandable, explain how children and their legal guardians can make requests, read the resulting information, and explain accessible routes of redress or for correction (for example in child friendly language where necessary). It is insufficient to post a privacy notice on a website to meet fair processing obligations, to be aligned with Article 8 of the Convention and paragraph 68 of the Explanatory Report, on transparency of processing.

e. To ensure consistency across different educational models in support of legal guardian and child rights to subject access and access to the educational record, in accordance with Article 9 (1)(b). legal guardians should be permitted to exercise these rights under Article 9, on behalf of the child in education, where the child, taking into account their level of capability, does not object.

f. Guidance is required by schools on subject access, and should include as appropriate and in accordance with national law, information on the recommended approach for schools when competent children may decline the sharing of their educational record with legal guardians, and for the provision of personal data to be made directly to a child rather than through subject access by a legal guardian.

g. Transparency to a child and their legal guardians should be supported by the proactive provision of information. Data Protection Impact Assessments demonstrate the intentions the start of a data collection process. Subsequent statements on the data processed, "data usage reports" should be made available on request, and on an annual basis, to each data subject or their legal guardian where the child does not object. These should demonstrate that what children were told would be done with their data in privacy notices, is what happened in practice, for the full lifecycle of processing.

h. Personal data retention and destruction notification should also be introduced as routine across the education sector, so that transparency information can be proactively provided about data processing, when a child begins, during and leaves each stage of compulsory education or each setting (across all children's ages, in nursery, primary, secondary, further and tertiary education).

i. Representation of child data subjects to supervisory authorities (Article 18) by third parties should be made easier and strengthened. Member States may provide under Article 13 for extended protection, that anybody, organisation or association independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the competent supervisory authority and to exercise the rights referred to the Convention if it considers that the rights of a data subject have been infringed as a result of processing.

j. Judicial and non-judicial sanctions remedies for violations of the provisions of the Convention under Article 12 of the Convention, should be made easy to access for a child, to further uphold children's rights under the UN Convention on the Rights of the Child (article 12). States that do not already have provision for collective complaints such as class actions and public interest litigation, should introduce these as a means of increasing accessibility to the courts for large numbers of children similarly affected by business actions, in cooperation, and with mutual assistance between supervisory authorities (Articles 15, 16, and 17(3)).

k. Where regulatory routes have already been exhausted, child litigants who bring a judicial case founded on the Convention 108 should be shielded from court cost orders, to benefit, whatever his or her nationality or residence, from the assistance of a supervisory authority within the meaning of Articles 15 and 18, to exercise his or her rights under this Convention.

2. Recommendations for data controller

2.1 Recommendations on processing in practice for educational settings

a. Procurement and legislation must respect the UN General comment No.16 (2013) on State obligations regarding the impact of the business sector on children's rights.[2] For example, 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.

b. Authorities and companies must meet their joint responsibility to respect the rights of the child in the digital environment and ensure that processing is safe, fair and transparent, regardless of complexity. If data processing is too hard to explain, to meet transparency obligations under Article 8 of the Convention, processing may not be suitable for processing using children's data for interventions, or that may infringe on their fundamental human rights or freedoms, or with significant effect.

c. Vendors should support the assessment of their suitability for processing school children's data, through an approved code of conduct or certificate, aligned with the Convention, Article 14, 3(b); or under Article 40 of GDPR.

[2] 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

d. Recognising that specific attention shall be given to the data protection rights of children and other vulnerable individuals, education authorities shall ensure that school staff are trained with respect to their rights and responsibilities in the course of their employment, regards data processing. Continuous professional development should ensure adequate capability to understand their role, in the exercise of object and purpose of the Convention and the activities set out in Article 2.

e. Each party shall ensure adequate levels of training, resources and the capability in relevant staff, to carry out due diligence aligned with Article 10, required during any procurement process, including an understanding of appropriate technical and organisational measures, and ethical and privacy impact assessments, before the introduction of new policy or technology that will result in the processing of children's data in education.

f. Recognising that not all educational institutions are schools, all parties must address teachers' or equivalent staff role in due-diligence and procurement of tools that process children's data, to ensure respect for a child's or legal guardian's rights as part of the decision-making over the introductions of any tool regardless of whether it is purchased, or freeware.

g. Data controllers should recognise that children cannot freely consent to the use of third-party services in particular where the power imbalance is such, in an education setting or public sector, that it cannot be freely refused without detriment.

h. Children and legal guardians must be offered a right to object to data processing in accordance with Article 9 (1)(d).

i. Objection to data processing for marketing purposes should lead to unconditional erasure or removal of the personal data covered by the objection.

j. In line with Article 9(d) the right to object at any time, to the processing of personal data concerning him or her, advertising should not be considered legitimate grounds for the processing that override students' interests or rights and fundamental freedoms. Children's education should be free from commercial exploitation to enable their full and free development, with respect for their human rights and fundamental freedoms, as enshrined in the UN Convention on the Rights of the Child.[3]

k. Schools have a responsibility to maintain a suitable level of alternative provision of education without detriment to the child, should families or the child exercise the right to object, as remedy, in accordance with Article 9 (1)(f).

l. In line with Article 9(d) the right to object at any time, to the processing of personal data concerning him or her, retention of a permanent record in any format, for the purposes of data analytics and product development should not be considered

[3] 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.

legitimate grounds for processing that override a child's interests or rights and fundamental freedoms.

m. In support of the principles of purpose limitation and minimal data retention, school agreements should prohibit processing personal data by third-parties in order to render it de-identified or anonymous with the purpose of retention and re-use beyond the purposes of the school, or the legal guardian or child's reasonable expectations.

n. Data processing agreements with terms and conditions that the school may not change, may remove the discretion of a school to limit the data that may be extracted by a company, or its processing method and purposes. Such terms are more likely to result in data processors taking on the role of data controller. Commercial vendors to public education providers should enable schools to change the terms and conditions in standard contracts, and have the ability to object without penalty, in the event of a new business policy, or changes such as a company takeover. Companies must inform schools of changes in terms and conditions, with a fair notice period to ensure a suitable business transition and providing the opportunity to cease processing.

o. Educational settings should carry out and publish a setting level, data protection audit report, to demonstrate their accountability and transparency of data processing with third-parties, as well as a register of the recipients to whom the educational setting has given personal data (such as to administrative and e-learning tools). Transparency should be further supported through the proactive publication of data protection impact assessments, privacy notices and any amendments to terms and conditions over time, to report on any breaches, and share any audit reports carried out of vendors or processors.

p. Controllers and processors must not sell children's personal data, collected in the course of their education, or reprocess it for the purposes of selling anonymised or de-identified data, in accordance with the principles set out in the Convention, aimed at protecting data subjects and also as mechanism for enhancing their trust.

q. Consistent with member States' domestic law, implement clear codes of practice for individuals where there is an expectation of access to school software through personal electronic devices, by staff or children. It should clarify appropriate uses, limitations and any consequences of using a personal device – in particular where software or mobile applications are installed.

r. To reduce the risk to the rights and freedoms of a child from a permanent single record, children should be provided with a "clean slate" of commercial or third-party storage of data related to them beyond their school, upon moving into adulthood should. Exceptions for compatible use, where lawful retention and appropriate safeguards are as provided for in law, under Article 5, and where in the direct best interests of the subject.

s. Schools should retain only pupils' records on leaving the educational establishment which are necessary and proportionate under Article 5, and in support of Article 7(1),

in accordance with and ensure that third parties in particular without statutory functions, do not maintain a permanent record of the child or their behaviours.

t. Records should not be preserved in a form which permits identification for longer than necessary, in particular beyond the school, with regard to the provisions of Article 5 (4), Article 7(2), Article 8 (1) and Article 9, when such an exception is provided for by law, and respects the essence of the fundamental rights and freedoms of the child and constitutes a necessary and proportionate measure, necessary in a democratic society for the purposes of Article 11.

u. Data linkage of the pupil record with other personal data should not be routine and must be communicated to the data subjects in advance of new processing, for purposes that are compatible with Article 5(3)(b) of the Convention. The data to which the pupil record are to be linked must also be made accessible to the data subject or their legal guardian. Data processing for similar purposes should have a privacy impact assessment, and ethics oversight where used for research purposes.

v. To ensure end-to-end transparency and accountability for data processing, educational authorities should maintain and proactively publish a school-level register of its data processing partners, such as vendors and subcontractors, as well as a transparency register of recipients of data, whether through access or distribution.

w. Each controller shall ensure transparency[4] of their policies on data processing, by drafting, maintaining and publishing their policies: on their data processing, including the legal basis and intended purposes of processing, retention and sharing of pupil records, data subject rights under Article 9, and the responsibilities of the data controller. Policies around professional confidentiality should also be published.

x. Controllers must ensure transparency of the technical and organisational measures in place for the processing of children's data after it has been given to processors or recipients, taking into account the duties regarding the protection of personal data at all stages of the data processing in accordance with Article 10(3). This obligation should be supported by routine publication by educational bodies about the processors and joint controllers they engage with; publishing data protection impact assessments, child rights and risk assessments, data sharing agreements, contract terms and conditions, and privacy notices, for the processing of personal data for which they are the controller. The processing by each party should be set out in contractual arrangements and be made publicly available, for example, online.

y. Controllers shall inform the data subjects of processing at the point of collection, during processing, and through the entire life cycle of the personal data processing, in a proactive manner, to meet transparency obligations under Article 8 of the Convention.

[4] WP29 Guidelines on transparency recommend if controllers are uncertain about the level of intelligibility and transparency of the information and effectiveness of user interfaces/ notices/ policies etc., in particular for children, controllers may test these, for example, through mechanisms such as user panels, readability testing, formal and informal interactions and dialogue with industry groups, consumer advocacy groups and regulatory bodies, where appropriate. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

2.2 Recommendations on the involvement of children and their legal guardians

a. To enable children and their legal guardians to understand their rights of Article 8(1)(e) communications about data processing must be in an intelligible form, appropriate for the competency of the child. Any chain of data distribution must be explainable and accountable at the point of collection, and in child-friendly language.[5]

b. Educational authorities should proactively inform school children and their legal guardians no less than annually, through the issue of an annual statement or within a reasonable period of time on demand, of the data processing by the institution, state, or private companies, listing every data controller and processor of the child's personal data processed through the school and by its contracted third parties, in order to enable the understanding needed to enact the data subject rights of Article 9(1).This should be made available through the school.

c. 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. A full copy of their record should be made available to the competent child or their legal guardian, including information about any ongoing requirements for data processing and retention, even after the child's education is complete.

d. On demand and upon leaving an educational setting, the educational authority as the data controller, must be able to provide a child with a statement describing the third parties to whom their personal data have been distributed, each retention policy, and expected destruction date. This should continue to be proactively made available at reasonable intervals, to the data subject, through the life cycle of the processing.

e. Public authorities should establish a default position of involving legal guardians in decisions before sharing their children's personal data, unless a competent child refuses such involvement or where sharing poses a risk to the child's best interest to ensure personal data shall be processed fairly and in a transparent manner aligned with Article 5(4)(a).

f. Parties shall recognise that data processing on the basis of free, specific, informed and unambiguous consent, where the data subject is a child, is impossible to obtain given the power imbalance between a public authority and a minor, except as an objection to assert the withholding of consent.

g. Legal guardians should be permitted to exercise the rights under Article 9, on behalf of the child in education, where the child, taking into account their level of capability, does not object. Opt-in is a more appropriate obligation than opt out, where a child or

[5] Paragraph 68 Transparency of processing: Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808ac91a

legal guardian's objection to processing is offered, to protect rights by design and default.

h. Schools cannot assume consent on behalf of legal guardians or children, to provide to third party providers, but rather must have an alternative lawful basis for both their own role in the data processing and ensure the validity of the lawful basis for processing by any recipient of the data collected by or on behalf of a school or educational authority, before its processing.

i. Parties shall provide that data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law, before a child's special category data, as defined in Article 6, may be shared for purposes beyond their direct care and education by the institution the pupil attends. If one legal guardian or the competent child objects, the data may not be shared.

j. Parties shall provide that data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law, before transborder flows of personal data and subject to appropriate levels of protection, according to Article 14 (3) and (4). If one legal guardian or the competent child objects, the data may not be shared.

k. Where data processing was carried out on the basis of the free, specific, informed and unambiguous consent given by the legal guardian of the data subject when the data subject was a child, the ability of the guardian to exercise lawful rights on behalf of a child, should be expected to expire when the competent child reaches the age of lawful maturity as laid down in law in the Member State. The consent process must transfer to and be requested of the data subject, the child of the legal guardian, to be able to exercise their rights as an adult.

l. Legal guardians should be asked for free, specific, informed and unambiguous consent before their own personal data are transferred to commercial education companies through the school system as part of the child's record, able to be refused without detriment.

m. On completion of compulsory education or when the child leaves one school to study at another school, or changes stage between primary, secondary, and further or higher education, authorities should be alert that the lawful basis of consent may no longer apply, where the child is no longer being educated or is in the direct care of that educational authority, and should seek to re-consent data processing on a regular basis, or have another legitimate basis for ongoing retention throughout the life cycle of the data processing.

n. Personal data outwith a school's scope include social media content from personal accounts and public fora. Such data from legal guardians, children or staff, should only be processed by schools with the consent of the data subjects, since this is outwith the school's statutory role and educational remit. Such processing may include parent-school association social media pages. Processing such information from a child's

access to services during school hours, should not form part of a child's permanent record or be retained without express purposes set out in law, in accordance with Article 11.

2.3 Recommendations on data use with automated decisions and profiling

a. The principle of Article 9(1)(a) of the Convention requires any data processing by any technology, to be explainable in a way that can be easily understood by a child.

b. Every individual shall have a 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).

c. Principle 3.5 of Council of Europe recommendation CM/Rec(2010)13 and explanatory memorandum[6], advises in principle, the profiling of persons who cannot freely express their consent be forbidden, especially, for example, adults with incapacity and children, within the meaning of the United Nations' Convention on the Rights of the Child. It is considered that such a prohibition in principle is necessary in view of the dangers of manipulation and negative discrimination represented by profiling in respect of these categories of individuals. The prohibition can be lifted by member states where profiling is used in the legitimate interests of the individuals concerned (for example, to obviate a particular danger of which these persons must be made aware, or to enable them to benefit from a form of assistance for which they have a specific need) or if there is an overriding general interest provided for by law and offering appropriate guarantees. Children's attainment should not be routinely profiled in order to measure systems, for example, for measuring schools or teacher performance management.

d. Where artificial intelligence is employed, the development and use must be assessed to ensure it should not be discriminatory, deepen the digital divide, and does not display or entrench bias. Any tool using data from children, requires data protection and privacy impact assessments, and child rights impact assessments[7].

e. Where data are used for automated assessment, prediction, or decision making, the process and information of the reasoning underlying data processing where the results of such processing are applied to them, should be transparent to educators and staff, learners, legal guardians and children. A right to object, to challenge resulting assessments and action, and to ask for a human decision instead should be offered proactively. Data subjects must have the opportunity to substantiate the possible inaccuracy of the personal data before it is used, the irrelevance of the profile to be applied to his or her particular situation, or other factors that will have an impact on the result of the automated decision, which may be particularly long-lasting for a child.

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

[7] 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

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 with the service buyer such as the school, but not the child since they cannot enter into a contract.[8]

2.4 Recommendations on biometrics

a. Good practice regarding children's biometric data processing, may include a requirement for controllers to register this processing explicitly with supervisory authorities in order for the authorities to be able to monitor such processing within their territorial scope, recognising the nature of sensitive data and recognising that specific attention shall be given to the data protection rights of children and other vulnerable individuals, in order to assist data subjects to exercise their rights under Article 18 of the Convention.

b. The use of biometrics in schools such as for biometric authentication for identity and remote proctoring shall only be allowed where appropriate safeguards are enshrined in law, in accordance with Article 6(1), aware of the risks that the processing of sensitive data may present for the rights and fundamental freedoms of the child, notably lifelong discrimination, and complementing those of the Convention.

c. 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 less invasive techniques of data processing exist, biometric data should not be routinely processed from children. Exceptions for use in support of people with accessibility needs, for example in screen eye tracking, for their direct benefit, may be processed with appropriate safeguards are enshrined in law.

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 behavioural data from a child, that may not be used only for verification of identity, but may be processed to influence physical or mental experience, such as in immersive virtual reality. Characteristics about voice, eye movement, gait, emotion and mood, and reactions to neurostimulation, may be processed for the purposes of influencing or monitoring a child's behaviour, their physical, or emotional developmental. Such data should be treated with similar care and sensitivity as biometric data under the Convention.

2.5 Recommendations for online content and communications data processing

a. Filtering and blocking Internet content, can be performed without monitoring and profiling individuals. If personal data are processed in order to protect children from online harms, all the usual data protection requirements must be satisfied before

[8] 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)

processing begins, such as identifying a fair and lawful basis for processing, ensuring that the processing is necessary and proportionate to the harm intended to prevent, and providing transparency information.

b. A measure which is "necessary in a democratic society" must pursue a legitimate aim and thus meet a pressing social need which cannot be achieved by less intrusive means. Such a measure should, furthermore, be proportionate to the legitimate aim being pursued and the reasons adduced by the national authorities to justify it should be relevant and adequate. Such a measure must be prescribed by an accessible and foreseeable law, which must be sufficiently detailed.

c. Awareness of more than data protection law is necessary in order for school staff to make an informed choice when considering online content and communications data monitoring of children and staff in schools. For example, Article 5 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 is devoted to the confidentiality of communications; Article 5(1) provides: '*Member States shall ensure the confidentiality of communications and the related traffic data [...] shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned*...' and, that the 'law' must, in effect, be '*adequately accessible and foreseeable, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct,*' to '*foresee its consequences for him,*[9]' '*to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail*'[10]

d. Principle 3.8 of Council of Europe recommendation CM/Rec(2010)13 and explanatory memorandum[11], recommends that, "*the distribution and use of software designed to observe and monitor use of a terminal or communication network not be permitted, as this would make it possible to collect data and use profiling methods without the data subjects' knowledge, unless expressly provided for by domestic law and accompanied by appropriate safeguards. For example, it is unacceptable that, as a result of security holes in software available on the market, applications may install themselves on an individual's computer or simply monitor all or selected uses of a terminal or network in order to build up user profiles*."

e. To be aligned with Article 3 of the Convention, processing of personal data must be processed lawfully, and 5(2)(a) requires it to be fair and in a transparent manner.

f. Systems cannot both meet the transparency obligations of data processing under the Convention, and also routinely monitor children's online content or communications with the intention of catching children out or for covert surveillance. This capability should be regulated in law due to the capacity for extensive intrusion into privacy and family life, risks to freedom of expression, and risks they introduce to the full and free

[9] European Court of Human Rights, judgment in *Leander v. Sweden* [1987] no. 9248/81, Series A no. 116, § 50

[10] European Court of Human Rights, judgment in *Margareta and Roger Andersson v. Sweden* [1992] no. 12963/87, Series A no. 226-A, p. 25, § 75.

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

development of a child, through their chilling effect. Processing activities for national security and defence purposes must be subject to applicable requirements in relation to effectiveness of independent review and supervision mechanisms.

g. The capability and use of video surveillance or webcams to covertly film or photograph a child without their knowledge, even as exceptional, should be considered prohibited in schools unless the requirements can be assured of Article 5 on legitimacy of processing, on security according to Article 7, and the rights and freedoms protected of a child, notably freedom of expression of Article 11(1)(b).

h. Controllers should transparently report to children and legal guardians, on no less often than an annual basis, on their accountability for transparency of individuals' data processing in accordance with Article 8(1)(e), and the means of exercising rights set out in Article 9. This may include considerations such as reporting filtering rates and content blocking. Any monitoring at child level should require a reporting obligation to report on the children's categorisation, data retention, access and distribution, logfile volumes and its content, error and correction rates and redress. At school level, a report should be provided to legal guardians and pupils on an annual basis, made available on request, and be reviewed to ensure practice complies with principles of necessity and proportionality, and to monitor capability, scope creep, and increase transparency of any potential discrimination of communities, in order to exercise individual rights to end unfair practice, and support redress.

i. Any targeted web monitoring of children's online content and communications data for the purposes of State countering violent extremism programmes identified in education, should require independent judicial oversight.

3. Recommendations for developers and manufacturers, and vendors

3.1 Recommendations for guidance in the context of edTech

a. The expected standard for the processing of children's data in the education sector should set a high bar by design, to meet acceptable quality levels and the rule of law, and data protection by design and by default. This must be supported by a combination of sector guidelines, statutory codes of practice and more sector specific enforcement by regulatory authorities.

b. Such standards may be set out in Codes of Practice and it is imperative that there is wide cooperation in their drafting with developers and industry, with education practitioners, academia, with organisations representing teachers and families, and civil society.

c. Developers must ensure that their own understanding of all the functionality of products they design to be used in the education sector, can be sufficiently explained to meet

regulatory and lawful requirements of the sector, and avoid creating a high investigative burden by design, inappropriate for schools and children.

d. Geolocation tracking in order to identify the location of use, the user, to target in app functionality, or for profiling purposes, should provide an indicator when the location tracking is active. Such profiles and history should be easy to delete at the close of a session. This should not be necessary to transmit to an indefinite number of persons.

e. Expectations of respect for the principles of data protection by design and default should include using design that does not incentivise children with features that may encourage children to provide unnecessary personal data or to lower their privacy settings.

f. 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.

g. Data processing 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. Data analytics 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.

h. Since children merit special protection, additional weight should be given to Article 12 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 adequacy framework.

i. Processing data in educational software tools (edTech), should not be permitted to serve or target behavioural advertisements, for real time bidding advertising technology (adTech), or for in app advertising, to serve children or families marketing for product upgrades or additional vendor driven products.

j. Provisions of lawful design and data processing contracts, at the time of the procurement must also continue to apply after the purchase, merger, or other acquisition of an operator by another entity, or have a sufficiently fair communication period for change of terms and right to alter or object to new conditions, or make such changes an automatic reason for end of contract and withdrawal of all client data on request.