15 November 2019 T-PD(2019)06BISrev

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: Challenges and Possible Remedies

Recommendations Summary

by Jen Persson, Director of defenddigitalme.

Directorate General of Human Rights and Rule of Law

Recommendations Summary

Recommendations on consent and contract

- Adequate levels of knowledge and the ability to carry out due diligence during the procurement process, including ethical and privacy impact assessments are needed at the appropriate point of decision-making before introduction of technology.

- Commercial vendors to public education providers should be banned by contract from significantly changing terms and conditions for apps and platforms without re-informing schools, children, and parents, and providing the opportunity to cease processing, in a suitably appropriate timeframe.

- Advise school children and families annually of their rights that apply to processing by the institution, state, or school children's data handled by private companies and issue a notice of every contracted third-party data processor.

- Schools must offer a right to object to the use of a third-party provider,

- 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 to the product.

- Written consent models should persist for health data, data re-use for non-educational purposes, such as before the distribution of personal data to any employer, third-party recruiter, in press, or for research purposes.

- Train and retrain school staff with respect to the requirements and ensure continuous development training.

- Draft and maintain policies with regard to consent and confidentiality, retention and sharing of pupil records that pertain to the disclosure of information for health and welfare concerns.

Recommendations on children’s agency

- 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. It is for public authorities to provide sufficient information and in such accessible manner, to adequately support children’s capacity for informed understanding.

- Companies must meet their responsibility to respect the rights of the child in the digital environment and ensure that processing is safe, fair and transparent regardless of product complexity. If it is too hard to explain, processing should not be deemed suitable for applications using children’s data for interventions, that may infringe on their fundamental human rights or freedoms, or with significant effect.

- States and other stakeholders should ensure that children are made aware of how to exercise their right to privacy and data protection, taking into account their age and maturity and, where appropriate, with the direction and guidance of their parents, carers, legal guardians or other persons legally responsible for the child in a manner consistent with the evolving capacities of the child. (The CoE Guidelines on Children in the Digital Environment Recommendation CM/Rec(2018)7 (2018)) Further support should be offered if it comes to seeking redress. (See I.5)

- Agency should be restored to children and the imbalance of power reduced by requiring that data that leave a setting are not by default identifiable, and identifiable data remains on site, except after assessment of necessity and with accountable approval. Any daisy chain of data onwards distribution must be explainable at the point of collection.

- Apps and platforms should not include direct marketing, or in-product adverts and marketing, in particular using user data to target or measure engagement.

- Minimum viable data should be retained at the point when a child leaves education, and only in the child's best interests, such as to demonstrate attainment, safeguard their future rights of access to necessary and proportionate personal data and to meet statutory obligations. A full copy of their record should be made available to them, with ongoing requirements for data usage and retention reporting, throughout the data life cycle.

Recommendations on the permanent single record

- To support the principle of data minimisation, and with exceptions for lawful retention where in the direct best interests of the child:
    - Children should be ensured a free and unmonitored space of development and upon moving into adulthood should be provided with a "clean slate" of any public or private storage of data related to them.
    - Children's formal education should be free from commercial exploitation and other self-interests, and
    - The integrity and agency of future generations should be ensured by providing children with a childhood where they can grow and learn untouched by unsolicited monitoring, profiling habitualisation and manipulation for companies' future purposes.

- Schools should ensure that pupils' records on departure which are necessary and proportionate to retain, are retained locally but that third parties and commercial vendors in particular without statutory functions, do not maintain a permanent record of the child or their behaviours.

- National records should not be retained at individual, identifying level.

- Children must have a right to restriction of disclosure of their school records to private companies during their direct education and for indirect secondary purposes.

- Sensitive data that may not meet the criteria of sensitive data or special category data under data protection law terms, ie: school records of behavioural history (aggression but

not criminal violence) or family factors such as wealth indicators, should be suppressed by default from distribution for purposes beyond the direct care of the individual

- In assessing cases of such data processing, there is significant imbalance of power between the school authorities and child, and discussion should be held with families before third-party distribution, with the default position as to ask for agreement under opt-in. Opt out is an insufficiently robust mechanism of protection in particular since so much data can be extracted from schools in an automated fashion.

Recommendations on hidden data issues

- Recommendations must include a prohibition on controllers/providers and their sub processors selling children's personal data collected in the course of their education, including a ban on reprocessing for the purposes of selling the reprocessed data or products built upon it.

- Data linkage should not be routine, and must be communicated to the data subjects in advance of new processing, for strictly purposes that are compatible with Article 5(3)(b) of the Convention. The data to which the education data are to be linked must also be made accessible to the data subject. Data processing for similar purposes should follow privacy impact assessment and have ethics oversight where used for research purposes.

- Ensure high standards of consumer protection, privacy, security, and data protection laws are applied to educational apps and platforms consistently and enforced in cooperation, by working together transnationally. (Articles 15, 16, and 17(3))

- Special educational needs data must be recognised as special category data.

- Special educational needs data should be processed accordingly as special category data and require a high bar of exemptions from data protection law, before it could be repurposed from school information management systems or apps. Consent for sharing for direct purposes should allow the same ethical and professional standards as health data, and should be given due recognition as confidential data.

- The data minimisation principle in data protection must be respected not only at the point of collection. The minimum viable amount of data should be collected for narrow purposes.

Recommendations on parental involvement

- Public authorities should establish a default position of involving parents 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.

- Introduce a parental right to object to secondary indirect purposes of data processing, those beyond which a child or parent does not expect their data are processed in the course of their education by the public body. (Indirect uses)

- Consent should be recognised as an exceptional lawful basis for data processing, and not appropriate for routine tasks required of compulsory education. This means that schools cannot assume consent on behalf of parents or children, to provide to third party providers, but rather must have an alternative lawful basis for third-party data processing.

- Schools should ensure active freely given consent is required for secondary or indirect purposes of data processing, those beyond which a parent would expect their child's data are processed in the course of their everyday direct education, provided for enrolment, or in the admissions process.

- Informed parental consent should be required before a child's special educational needs data may be shared outside their direct care and education by the institution the pupil attends.

- Informed parental consent as the lawful basis provided by the institution the pupil attends for data processing, to third parties, should expire upon the child leaving education regardless of age. This may mean on completion of compulsory education or when the child leaves one school to study at another school, or changes stage (Primary, Secondary, College).

- The lawful basis must transfer to, and be asked of the child on reaching the lawful age of majority.

- Parents should be asked for consent before their own personal data are transferred to commercial education companies through the school system, and consent must be informed and freely given, and able to be refused without detriment. For example, parents should not find that their email address has been provided to set up a Platform Classroom account and link a child's record to theirs, where data will leave the school.

- Social media content from personal accounts and public fora, from parents, children or staff, should not be surveilled by schools for any purpose, outwit the school's statutory role and remit, and where there is no lawful basis for the processing of personal data. Even where schools fear reputational institutional risk, processing such information should not form part of a child's permanent record.

Recommendations for schools and staff

- Staff must recognise that children cannot freely consent to the use of third party services in particular where the power imbalance is such that it cannot be refused, or easily withdrawn. Schools must accordingly address teachers involvement in product due-diligence and procurement, to ensure respect for child/parental rights in all processing.

- Basic teacher training and professional development should offer mandatory content on basic data protection, privacy, and other related children's rights.

- School agreements should prohibit processing personal data by third parties / providers in order to render it de-identified or anonymous for re-use for their third-party purposes and retention, beyond the purposes of the school's reasonable expectations and purposes, in support of the principles of purpose limitation and data retention.

- 'Click—Wrap' agreements — agreements about terms and conditions that the company or product vendor does not permit the school or user to change — remove the discretion of a school to control which data may be extracted by a company. These should be prohibited.

Schools must be able to keep control of the data about their children by preventing a provider from changing its Terms and Conditions without a school's ability to refuse and continue service for a fair business transition period.

- Procurement processes should ensure adequate due diligence including risk assessment, and the maintenance of a school-level register of data processing vendors and sub-contractors, as well as a data register of third party data access and distribution.

- Schools should remain the data controllers and third parties as processors. The boundaries of this should be set out in contractual arrangements and be made publicly available.

- The challenges of balancing risks posed by data distribution for reasons of data security, retention costs, and growing use of cloud storage by default, should be balanced together with a general principle that children's personal digital footprint should not leave the school.

Recommendations on reducing the investigative burden

- Commercial vendors to public education providers should be banned from changing terms and conditions for apps and platforms in the event of a new business policy, or owner, without re-informing schools, parents, and children, with a fair notice period (i.e. one month) and providing the opportunity to cease processing.

- Stakeholders involved such as vendors, industry, marketing and advertising should prove they have an approved code of conduct or certificate (Fr example, as per Convention 108+, article 14, 3(b); or under Article 40 of GDPR).

- Data Protection Impact and any associated Risk Assessments, including links to third party privacy notices, should be published as part of the due diligence before a new technology or product is introduced to a school.

- On demand and on leaving an educational setting, the body must be able to provide a child with their data usage report, describing the third parties to whom which personal data have been distributed, each retention policy, and expected destruction date.

Recommendations on representation and remedy

- It must be made easier for schools to adequately represent pertinent data subjects rights.

- Schools should be supported by guidance of data protection authorities when creating standardised subject access rights as relates in particular to email

- Representation of child data subjects to supervisory authorities (Article 18) by third parties should be made easier and strengthened. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to

exercise the data subject rights on his or her behalf, and to exercise the right to receive compensation on his or her behalf where provided for by Member State law.

- Member States may provide 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. 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.

- 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.

- Subject access rights should be standardised for children to change the inconsistency between different school models of support of parental and child rights to subject access and access to the educational record and the wide variety of school information management systems (stored in schools or offsite on companies' cloud servers which are commonly abroad), platforms and apps in use. Guidance is required by schools, and as appropriate to member state law, on when competent children may decline the sharing of their educational record with parents and for the provision of personal data to a competent child rather than parent via subject access.

Recommendations on data use with automated decisions and AI

- The principle of Article 9(1)(a) of the Convention needs developed fully into guidelines for education, and in ways that are rights respecting and understandable for children. Any AI or profiling should be explainable, and in a way that can be understood by a child.

- The High Level Expert Working Group on Artificial Intelligence (HLEG-AI) proposal should be adopted into guidelines and legislation: "Children should be ensured a free unmonitored space of development and upon moving into adulthood should be provided with a "clean slate" of any public or private storage of data." This should be the general principle as is Data Minimisation, and retention beyond the school years should be permitted exceptions with clear legislative exemption, rather than the general practice.

- Any product testing and pilots involving children permitted under member state law, should be treated in the same manner as a health research trial requirement ethics committee oversight, privacy and risk impact assessment, opt-in consent, and for non-participation to not be at the detriment of the child.

- Profiling should only be carried out in certain narrow circumstances (e.g., to protect a child's vital interests) and children's attainment should not be routinely profiled in order to measure systems ie. for benchmarking schools or teacher performance management.

- Where AI is employed, the development and use must be assessed to ensure it should not deepen the digital divide and does not display or entrench bias. Any use with a child or using data from children, must require data protection and privacy impact assessments.

- Where data is used for automated assessments or decisions which affect learners beyond the narrow confines of the educational experience provided by the platform, this process should be transparent to educators, learners, and parents. The latter should always be provided the right to object to use, and to challenge resulting assessments and decisions.

- Personalisation of content may (but does not always) constitute an intrinsic and expected element of certain online services, and therefore maybe regarded as necessary for the performance of the contract with the service user in some cases. (EPDB, Guidelines 2/2019) It should be clear however, that children cannot enter into a contract with third parties. Any service should be able to be provided without personalisation through profiling, and using methods that do not involve excessive data processing, within users' reasonable expectations, without detriment for those who object to such learning systems.

Recommendations on biometrics

- Controllers of children's biometric data should be required to register this explicitly with supervisory authorities.

- Biometric data definitions should expand to recognise personal data collection not only for verification of identity, but for use to influence physical or mental experience, such as physical attributes and experience in immersive virtual reality; voice, eye movement, mood, mental activity, polygenic scoring, reactions to neurostimulation, and data for the purposes of emotional developmental influence, nudge and change.

- Prohibit the use of facial detection and recognition in education, among other biometric data processing of children, for insignificant routine activities, with exceptions for use in support of people with disabilities, for example in screen eye tracking for their system access and for their direct benefit.

- Biometric data collection should remain within the educational setting and not be made available for internal or external security purposes or crime prevention.

- Respect for the Rule of Law must continue to be a leading principle in any developing standards. These may want to consider alignment with forthcoming standards of processes for AI.

Recommendations for data processing on safeguarding

- The use of web monitoring a child that builds personal profiles should end, and be used for generically filtering and blocking content, not monitoring individuals. Systems should not be intended to catch 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, to freedom of expression, to a full and free development through their chilling effect.

- Transparency duty: Commercial companies providing child monitoring services should be regulated and required to transparently report on an annual basis. This may include corporate considerations such as filtering rates and content, blocking and monitoring capability expansion, monitoring and blocking appeal routes. Any monitoring at child level should require a reporting obligation to report on children's profile categories, data retention, access and distribution, logfile volumes and content, correction rates and redress. At school level, a report should be provided to parents and pupils on an annual

basis, made available on request, and be regularly reviewed to ensure practice complies with principles of necessity and proportionality and increase transparency of any discrimination and bias.

- Fairness: To ensure children and young people are informed about their data processing before it begins, schools and colleges should provide pupils, parents and staff with adequate information, tailored for different age groups, to understand how their online activity is monitored and recorded, and that and how they can be tracked, profiled and reported to third-party agencies and bodies. Before being asked to opt-in to Home-School IT agreements, pupils and parents must be informed how systems work and of its foreseeable consequences. Requirements should be set out in a Statutory Code of Practice.

- Targeted home web monitoring of children for the purposes of State countering violent extremism programmes identified in education, should further require judicial oversight.

- The capability and use of webcams to photograph a child without their knowledge should be banned in schools. It is deeply invasive and impossible to enable for only the rare and exceptional need for individuals, but not open it up to misuse for many.

- States should ensure that the processing of special categories of data, which are considered sensitive in accordance with Article 6 of the Convention, such as genetic data, biometric data uniquely identifying a child, personal data relating to criminal convictions and related security measures, and personal data that reveal racial or ethnic origins, political opinions, religious or other beliefs, mental and physical health, or sexual life and orientation, should be prohibited and only be allowed for exceptions, where appropriate safeguards are explicit, transparent, and enshrined in law.

- Camera use should never be covert. Data should be collected locally and retained for the minimal amount of time that is necessary and proportionate.

Recommendations on school transparency

- Fair processing notices must be tailored to children in education. It is insufficient to post a privacy notice on a website to meet fair processing obligations.

- Subject Access Requests about children must be tailored to them in how they can make requests, read the resulting information, and have accessible routes of redress.

- To close the loop with Data Protection Impact Assessments at the start of any data collection process, subsequent data processed reports, “Data usage reports” must be made available on request, and on an annual basis, to demonstrate that what children were told would be done with their data in privacy notices, is what happened in practice, for the full life cycle of the data processing.

- Data retention and destruction plan notices should also be introduced as routine, when a child leaves an educational institution, and completes each stage of compulsory education (nursery, primary, secondary, further, Higher).

- Educational settings should publish an annual 12-month school-level data protection audit report including a register of third party personal data distribution, data protection impact assessments, provision of privacy notices and any significant amendments, to report on any breaches, and any audit reports carried out of vendors or pupil data users.

Recommendations for guidance for developers in the context of edTech

- 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. This must be supported by a combination of sector guidelines, statutory codes of practice and more sector specific enforcement by regulatory authorities.

- 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.

- 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.

- 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.

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

- 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 parents and educators.

- 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. 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.

- 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.

- Processing data in educational products, should not be permitted to serve or target behavioural advertisements, for real time bidding adTech, or for in app advertising, or child or parental marketing for product upgrades or additional vendor products.

- Provisions of lawful design 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.