Contribution from defenddigitalme to the evaluation of the GDPR (Article 97)

About defenddigitalme

defenddigitalme is a call to action to protect children's rights to privacy. We are teachers and parents who campaign for safe, fair and transparent data processing in education, in England, and beyond. We advocate for children's data and digital rights, in response to concerns about increasingly invasive uses of children's personal information.

Defenddigitalme
April 2020

defend|digital|me

Summary

1. We submit a response in order to raise awareness of the particular needs of children, as well as young adult learners with additional vulnerabilities, such as those with special educational needs and disability. Our focus is on children's personal data in an educational context.

2. As an estimated 90% of the world's student population are affected by school closures[1] at the time of writing in the COVID-19 pandemic, technology is playing a vital role worldwide. Some commercial tools enable the international delivery of essential information, connecting school communities outside the classroom and may send children's personal data into the cloud —a term with little meaning to a child, and may include servers in-, and/ or outside the EU. Others provide platforms[2] for sharing educational materials that may be accessible without geographical borders via the Internet, or offer vital alternative means and modes of Assistive Technology and augmented communications, supporting the rights of those with disabilities[3] and collecting deeply sensitive special category data about mental health, and well-being.

3. Harms to children's privacy, dignity, free expression, and their UNCRC rights to full development and human flourishing, can result from various aspects of data processing.[4] There remains little evidence that specific instruments to safeguard children's rights in relation to dataveillance have been developed or implemented, and further attention needs to be paid to these issues. (Lupton, Williamson 2017)

4. For a variety of motivations, there is a rapid growth of international actors and emerging technologies in the multi billion dollar global edTech market[5], driven not only by angel investors and tech accelerators in US and UK[6] English language markets, but across the world. Foreign transfers of learners' personal data from the EU to third countries, the U.S., Australia, Hong Kong and China[7] in particular, are common in educational technology (edTech). In 2018, Chinese startups received over 50% of all the capital invested by venture capitalists in edTech worldwide. (Forbes) Some U.S. owned companies have U.S. servers because that is their headquarters, others because they want support staff to have real-time access to children's personal data, internationally,[8] 24/7, every day of the year.

[1] UNESCO COVID-19 Educational Disruption and Response https://en.unesco.org/themes/education-emergencies/coronavirus-school-closures
[2] UNESCO list of National learning platforms and tools (accessed March 28, 2020) https://web.archive.org/web/20200325181822/https://en.unesco.org/themes/education-emergencies/coronavirus-school-closures/nationalresponses
[3] UN Convention on the Rights of Persons with Disabilities (UNCRPD) Article 24 https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities/article-24-education.html
[4] Lupton, D. and Williamson, B. Lupton, D., & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. *New Media & Society*, *19*(5), 780–794. https://doi.org/10.1177/1461444816686328 (reference in paragraph 1.6)
[5] UNICEF, Discussion Paper Series: Children's Rights and Business in a Digital World (p5) Privacy, Protection of Personal Information, and Reputational Rights https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf
[6] EDUCATE https://educate.london/
[7] Why Is China The World's Leader In Edtech? (Forbes) 2018 https://www.forbes.com/sites/ricardogeromel/2019/04/05/why-is-china-the-worlds-leader-in-edtech/
[8] https://www.smoothwall.com/international/ and Internet monitoring of all content typed by children on their personal devices including passwords, counselling services and offline documents 02:55 https://www.youtube.com/watch?v=N7lEi5yGpYY

5. The implications for the child and society of the lack of meaningful regard for data protection for children are staggering. In the words of two U.S. based education companies CEOs':

> ***"Privacy went out the window in the last five years. For the good of society, for protecting kids."*** School safeguarding software company Gaggle CEO, Jeff Patterson (2019)[9]
>
> ***"the human race is about to enter a totally data mined existence, and it's going to be really fun to watch...the world in 30 years is going to be unrecognisably data mined...education happens to be today, the world's most data mineable industry– by far."*** Educational Platform Knewton (now Wiley) former-CEO, Jose Ferreira (2012)[10]

6. The aspects of data processing connected in their lawfulness and adequacy on other aspects of the Regulation are difficult to adequately assess for only this remit:
    a. *(a) Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of the Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC;*

       (b) Chapter VII on cooperation and consistency in particular cover the issue of international transfer of personal data to third countries (Chapter V of GDPR), with a special focus on existing adequacy decisions, and the cooperation and consistency mechanism between national data protection authorities (Chapter VII of GDPR).

   without also assessing other areas that need further attention, such as the relations between consent and other grounds for lawful processing: Clarification in Art. 6(1)(1) GDPR on consent as regards children needs further attention, in particular when it regards children's disempowerment in relations to public authorities and their commercial partners in compulsory state education.

7. For example, most educational apps' terms and conditions set out that they process on the basis of consent. This is because their processing goes beyond the boundaries of what is necessary and proportionate for schools' own needs. But as set out by the UK regulator, the ICO, children cannot freely consent to the use of such services in particular where the power imbalance is such that it cannot be refused, or easily withdrawn. "*Public authorities, employers and other organisations in a position of power may find it more difficult to show valid freely given consent."*[11] There are also fundamental problems with child/parental consent and competency, which should be subject to more research and attention.

---

[9] *Schools Are Deploying Massive Digital Surveillance Systems. The Results Are Alarming*, Education Week (July 8, 2019) reporting from interview with school safeguarding software Gaggle CEO Jeff Patterson https://www.edweek.org/ew/articles/2019/05/30/schools-are-deploying-massive-digital-surveillance-systems.html

[10] Quotes source: YouTube channel of the Office of Educational Technology at the US Department of Education. https://www.youtube.com/watch?v=Lr7Z7ysDluQ Knewton, an adaptive learning company that has developed a platform to manage educational content, has developed courseware for higher education https://www.knewton.com/ It was bought by Wiley in 2019.

[11] ICO on consent https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

8. As it is currently set out in the WP29 Guidelines on Consent under Regulation 2016/679[12] (and endorsed by the EDPB) the term 'information society service" in the GDPR and definition of "offered directly to a child", with reference to Article 4(25) GDPR to Directive 2015/1535, may be understood not to apply to online tools that a child uses in school, or that are managed via school contracts. However, they collect children's personal data during the bulk-registration process, and during the use of the app. There is no genuine consent process, yet the personal data collected are processed by companies in third-countries, as if there were.

9. Age verification should not lead to excessive data processing however it is common for business models to be based, not on the informed consent of the child, but promoting the absence of the need for a parent to give consent from 13,[13] and therefore removing protections for the child 13+.

10. We suggest for example, consideration should also be given to

a) the exclusion of consent as a child as a lawful basis for processing special categories of personal data according to Art. 9(2)(a) of GDPR to third-countries, since it is currently serving only to enable manufactured exploitation of children's personal data. Other lawful bases must demonstrate necessity and proportionality, which are often avoided if 'consent' is sought.
b) the exclusion of consent as a child as a lawful basis for the processing of personal data for automated individual decision-making.
c) more obligations to explain to children and families and their data processors, what genuine consent means and why for example the adTech sector and data brokerage businesses do not obtain it even where data are embedded in edTech apps or school data linkage, and therefore process children's personal data without lawful basis, which should be subject to easy-to-access enforcement and rights to redress.
d) Assessment of the criteria and Codes of Practice are required to define 'significant effect' with adequate consideration given to the developing nature of childhood and the added vulnerability to persuasion and significance of behavioural manipulation
e) Additional weight should be given to the right to object to processing in third countries and redress, where personal data are collected during childhood.
f) Incorporation of an obligation for special consideration of the fundamental rights and interests of children in the context of data protection risk assessment and the nature of child rights measures taken into account in a data protection impact assessment.
g) The aim of recital 38(2) in GDPR should be transferred to the articles and ban the use of children's personal data for the purposes of marketing or profiling
h) The consistent universal application of Article 80(2) to provide routes of representation and redress. This should be rectified and made compulsory.

[12] Guidelines on Consent under Regulation 2016/679 (wp259rev.01) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
[13] How Google Accounts work when children turn 13 (or the applicable age in your country) https://support.google.com/families/answer/7106787?hl=en&ref_topic=7336731

1. Transfer of personal data to third countries or international organisations

Further attention is needed regarding third country transfers and international organisations, with a wider range of articles, as regards making the recognition that children have an additional vulnerability an actionable reality when their personal data are processed. Such topics should be both addressed in sector specific Code of Conduct, as well as broader Codes for the processing of children's personal data:

- Article Article 25(6) (data protection by design and default) including
    - Article 5(1)(b) (purpose limitation);
    - Article 13 (right of information);
    - Article 15(3) (right to have a copy of one's personal data);
    - Article 33(1) (data breach notification);
    - Article 37(7) (notification of the data protection officer);
    - Article 41 (accreditation);

- Articles 58(2)(b) (competences of the supervisory authorities); and cooperation on 97(2)(b) (sanctions).

2. Recommendations

2.1 Prioritise privacy in the rights of the child in the digital environment across the public sector, where processing is part of public-funded activity.

Incorporate more of the Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment across the public sector as regards third country transfers.

2.2 Special category data are ineffectively protected in international transfer

a. Ensure high standards of consumer protection, privacy, and data protection laws are applied to educational apps and platforms consistently across the application of the GDPR for data under Art. 9(2)(a) GDPR.

b. Biometric data are processed and inferred routinely by commercial companies in education, such as eye movement on screen, voice, gait, brain and neural activity, as well as routine physical and mental health conditions, with little consideration given to the additional risks of third-country processing for children, where control is routinely lost forever.

2.3 Increase the transparency tools around commercial use and reuse of children's personal confidential data to children and their legal guardians.

a. Obligations should be made on controllers and processors of biometric data to have a duty to explicitly register processing biometric data with data regulators where it

concerns a child. Such processing should be expressly limited by necessity, and only where less invasive methods of processing are not available (for example for registering school attendance).

b. Children must have a right to restriction of disclosure to private companies to ensure their full development and adult flourishing. It should be possible for school records with behavioural history to be suppressed from distribution to and in third-countries; records such as violence, sexual misconduct, or drugs, and in particular the global trend towards the datification of children for the predictive purposes of countering violent extremism and terrorism, where the personal data are not transfered under for the purposes of criminal investigation, with adequate relevant judicial oversight.

c. Freedom of Information laws should apply to all non-state actors, companies and arms length government bodies, providing education and children's services to the state sector including third country processors. This is often not the case today, where such laws are limited to public services.

d. Transparency must be meaningful and demonstrate accountability. Third country transfers are opaque to children and their legal guardians. The adequacy of such decisions are self determined and schools cannot independently assess them. Whether binding corporate rules pursuant to Article 47 are met, can be specialist knowledge beyond most schools internal expertise. To facilitate therefore scrutiny by external bodies such as Supervisory Authorities and civil society, Public Authorities should be obliged to publish an open register of:
    - processors /subprocessors they engage processing children's data
    - a register of any commercially obtained sources of personal data collected for processing, or linkage with data provided by individuals in the course of their public sector interactions,[14] and update it on a regular basis. (i.e. Data brokers, third-party companies, social media)
    - Data Protection Impact Assessments, Retention schedules, and GDPR s36(4) Assessments with periodic fixed review to address changes
    - A duty on the controller to log all recipients of personal data; and an obligation to present the file to the data subject and where they do not have capacity, their legal guardians.

2.4. Restrictions are needed on high risk processing in school settings where data are processed both domestically and abroad.

a. Consider legislative limitations on the transfer to third countries of personal data obtained from surveillance of children via various biometric interactions -- which may not be exclusively processed for the purposes of identifying a child but that would enable it; facial detection and recognition, emotional manipulation, and neuro-/cognitive technology by commercial companies, or via webcam, voice recording, or gait and movement analysis, noting UN Special Rapporteur David Kaye's call for a moratorium on facial recognition technology[15] and the Swedish Data Protection Authority opinion and enforcement action in summer 2019[16].

[14] Cardiff Data Justice Lab Data Risk Scores https://datajustice.files.wordpress.com/2018/12/data-scores-as-governance-project-report2.pdf
[15] Moratorium call on surveillance technology to end 'free-for-all' abuses: UN expert
, (June 2019) David Kaye recommendations, United Nations Special Rapporteur on freedom of opinion and expressionhttps://news.un.org/en/story/2019/06/1041231
[16] Supervision pursuant to the General Data Protection Regulation (EU) 2016/679 – facial recognition used to monitor the attendance of students [DI-2019-2221]
https://defenddigitalme.com/wp-content/uploads/2019/12/facial-recognition-used-to-monitor-the-attendance-of-students.pdf

b. Personal data gleaned from children's personal data in behavioural science, neuroscience, personalisation via genomics, facial recognition and gait analysis, nudge, affective tech[17], and other emerging technologies should not be trialled in schools or sent to third countries. Any research studies should require ethical oversight and opt-in consent, without detriment.

c. Most state schools are poorly equipped to address the requirements under the Data Protection Act 2018 (and GDPR Article 25[18]) to minimise its data collections and ensure proper policy, technical and security measures to address excessive data collection and enforce retention (including at national levels or for children leaving compulsory school), limit unique identifiers, and ensure anonymisation. They do not have specialist staff in data protection or security. This creates a power imbalance for companies especially in international locations, and who rely on school staff lack of due diligence and capacity.

d. Children's data must not be used for purposes incompatible with the one that legitimised their collection and that the people were told about at that time. Non-educational purposes of historical national pupil data by State government departments (for example, the misuse of school records by the UK government for immigration enforcement) must end to protect a child's right to education and their right to private and family life.[19] New laws should not subsequently permit repurposing data collected in the past.

2.5 Introduce a non-commercial-use obligation on the re-use of children's personal data collected in education, that are transferred to third countries.

It is common for edTech to re-use personal data provided for the school / pupil's purposes of direct admin, teaching or communications,, for their own commercial company purposes; whether for in-app advertising, pitching at parents' emails for upgraded or sister products, or product development including new AI tools; chat bots, and virtual learning platforms. Children and their parents being captive addressees for marketing is mainly a consumer protection problem. But from a human rights point of view, it is the prior collection of personal data, and repurposing for indirect uses, which is problematic for privacy. Further uses of compulsory [access][20] data, misused to restrict 'undesirables', is already a reality.

2.6. Lawmaking[21] and procurement at all government levels, must respect UN General comment No.16 (2013) on State obligations regards the impact of the business sector on children's rights,[22] regards data protection and privacy

"a State should not engage in, support or condone abuses of children's rights when it has a business

[17] Dr Selena Nemorin, University College London, Affective capture in digital school spaces and the modulation of student subjectivities. Emotion, Space and Society, 24. pp. 11-18. ISSN 1755-458

[18] ICO Data Protection by Design and Default (Article 25)
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

[19] Timeline of Home Office access to pupil data in England for immigration enforcement purposes
https://defenddigitalme.com/timeline-school-census/

[20] King's College London has apologised to student activists who were barred from entering the university's buildings during a visit by the Queen in March, after an inquiry found security staff "overstepped their authority".
https://www.theguardian.com/education/2019/jul/04/kings-college-security-overstepped-authority-over-activists-during-queens-visit-inquiry

[21] Higher Education and Reserch Act 2017 and Regulations 2018/19
https://www.parliament.uk/documents/lords-committees/Secondary-Legislation-Scrutiny-Committee/Session%202017-19/Product%20safety/Defenddigitalme%20submission%20on%20%20Higher%20Education%20Act%20Regulation%202019%20v2.pdf

[22] Committee on the Rights of the ChildGeneral 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

role itself or conducts business with private enterprises. For example, States must take steps to ensure that public procurement contracts are awarded to bidders that are committed to respecting children's rights. State agencies and institutions, including security forces, should not collaborate with or condone the infringement of the rights of the child by third parties. ***States should not invest public finances and other resources in business activities that violate children's rights****."*

2.7 Machine learning and AI using pupil data, automated decision making, profiling, risk scores and prediction, must all have tight oversight across their lifetime use after any transfer to third country, and be understandable to public sector staff and families, with regular updates on the continued processing.

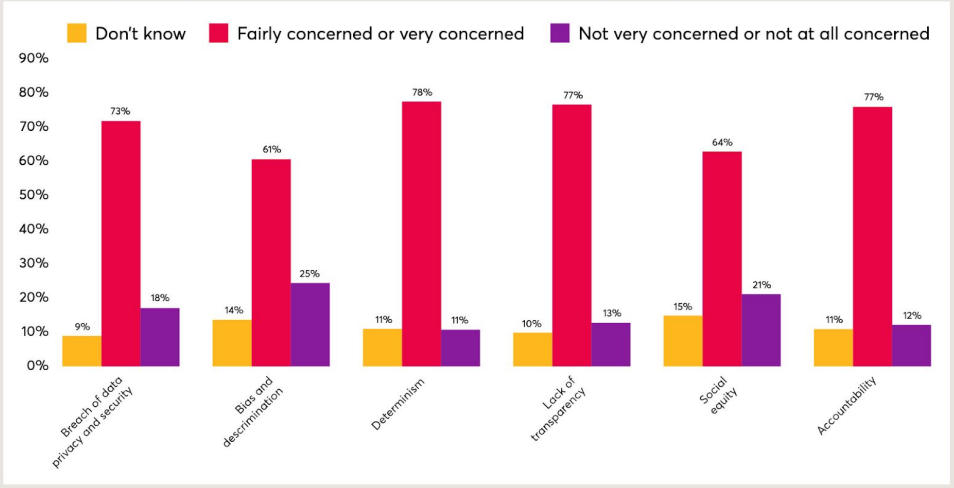
a. In June 2019, the High Level Expert Working Group on Artificial Intelligence (HLEG-AI) in their Policy and Investment Recommendations for Trustworthy Artificial Intelligence, proposed children must be better protected:

> "*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.*"[23]

b. There need be no conflict between privacy and innovation[24], yet some products in emerging fields, including machine learning and Artificial Intelligence infringe on rights. Legal guardians in the UK are concerned how this may affect their children including discrimination, bias and social equity. (Nesta, 2019)[25]

- 77% of parents with children aged 18 and under are concerned about accountability of AI decisions
- 77% are concerned about a lack of transparency
- 73% are concerned about breaches of data privacy and security

Figure 9: Concern of parents surveyed about potential consequences of the use of AI in UK schools



Source: YouGov. AI in schools. 2019. Survey commissioned by Nesta.

[23] Policy and Investment Recommendations for Trustworthy Artificial Intelligence (accessed July 1, 2019) (published June 26, 2019) https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence (permanent copy https://defenddigitalme.com/wp-content/uploads/2019/07/AIHLEGPolicyandInvestmentRecommendationspdf.pdf)

[24]https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/ Denham, E., The Information Commissioner3 July 2017, findings on Google DeepMind and Royal Free

[25] To obtain the perspective of parents on AI and education Nesta commissioned YouGov to undertake a survey of 1225 GB parents with children aged 18 and under https://media.nesta.org.uk/documents/Future_of_AI_and_education_v5_WEB.pdf Educ-AI-tion Rebooted? Exploring the future of artificial intelligence in schools and colleges

c. Artificial intelligence companies should not exploit children's data gathered in the course of compulsory education, for their own company product development yet this is what happens in many third countries where the child's personal data are processed for the purposes of the company, not the educational establishment or the child. Companies commonly retain children's personal data indefinitely with pseudonymisation adopted by the company as a poor replacement for anonymisation, for product enhancement.

d. With this 'anonymisation' completed, companies often continue to process children's personal data indefinitely and without their knowledge, into adulthood. While the harms may be at the moment, restricted to a breach of processing law and fundamental rights, the potential future effects on the future adult may not yet be apparent.

2.8 Cooperation and consistency of appropriate action are needed

a. The consolidation of the edTech market without due attention from Competition and Market Authorities, means that many companies operate internationally and control the personal data of millions of children from different countries.

b. Cooperation and consistency in particular on the assessment of breaches and the enforcement of rights, regards international transfer of children's personal data to third-countries, and by global companies that operate across many Member States is urgently required, with a special focus on existing adequacy decisions and binding contract terms. No child can fairly understand what these mean. There are decisions which may have ramifications for all member states yet no consistency of action so that good decisions fail to bring out the shift of power and systemic change required to protect children's data rights.

c. The cooperation and consistency mechanism between national data protection authorities (Chapter VII of GDPR) needs urgent action to enable supervisory authorities to co-operate globally to publish guidelines, monitor practice, and ensure compliance, and to recommend and promote only safe, fair and transparent products, ensuring education without exploitation.

2.9 Cooperation and consistency with and across third countries is needed

Cooperation and consistency in particular as regards children's data with third countries, must take into account the countries' own regulations and mechanisms, which could be outside the EU remit of the GDPR, however would serve well to support GDPR rights and enforcement. Cooperation on the basis of other mechanisms may be more effective than GDPR alone, for example the Convention 108+[26] including the Additional protocol to Convention 108 regarding supervisory authorities and transborder data flows (ETS No. 181) and further *Guidelines for Data Protection for Children in Education* (forthcoming 2020).

---

defenddigitalme.com
April 2020

[26] The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) https://www.coe.int/en/web/data-protection/convention108-and-protocol