Report Stage Briefing - Amendment 117

Code on processing personal data in education where it concerns a child or pupil

We welcome and invite support for amendment 117 in the name of the Earl of Clancarty.

It seeks to require the Commissioner to produce a code of practice, pursuant to GDPR Article 40(g), relating to the rights 40 (a)-(k) as specific to children (up to age 18 for purposes of GDPR except where stated in the Bill) and pupil (as defined by the Education Act 1996, who may be up to age 19). The obligations of schools and data controllers appropriate to children's age, type of education and capacity, need clarity and consistency.

Lord Clement-Jones said at Committee stage, [Col 1865], on Article 22 and safeguards, "*the provisions related to automated decision-taking should not be allowable in connection with children. That requires clarification*." Obligations specific to children's data, especially regards "solely automated decision making and profiling," and exceptions, need to be consistent, with clear safeguards-by-design where they restrict fundamental freedoms.

A code is needed a) because the safeguards are missing that GDPR requires in several places. Clause 13 of the Bill (automated decision-making authorised by law: safeguards), and 14 (exemptions) do not address the required safeguards of GDPR 23(1) for children, at all. Clause 9(6) and 15 (powers to make further exemptions) are inappropriately wide and as in our briefing at Committee stage we recommend their removal. b) edges of the definitions is unclear are many parts of the bill, on public interest and significant effect, and not clear for schools.

Clauses 47 and 48 of the Bill again take no account of children, for whom CCTV and IPTV capture facial images and in schools very commonly a range of other biometric data, and it is impossible in public and in educational spaces not to "manifestly make [them] public" as described in GDPR Article 9(e) but again the required safeguards of GDPR 9(g) have not been put into the Bill for children. A code should make child rights clearer.

A code should breathe life into the explicit recommendation of the Working Party 29 to create guidance on automated decision-making with significant effects and profiling in Recital 71, such a measure 'should not concern a child' and principle of Recital 38, that children "merit specific protection." The WP 29 wrote ***"Article 40(2) (g) explicitly refers to the preparation of codes of conduct incorporating safeguards for children;"***

For common case studies of profiling in education in England see our submission to WP29.[1]

Much debate has been around child protection, not their data protection. While integral to one another in online safety, these protections are also distinct from one another. Although the broader debate of ethical principle is outside this debate, some of the interpretative value judgements of Recitals specific to children under GDPR must be embodied in a manner understandable for everyone in a data ecosystem, if we are to see anything happen. If not, uncertainty and unwillingness to co-operate in a responsible and interoperable manner, will make the whole process of child data flows unworkable; and impossible for a child to manage their digital footprint.

1. Adherence to a code creates a mechanism for
    a. controllers and processors to "*demonstrate compliance with the legislation or approved certification mechanisms."* [GDPR Articles 24(3)]
    b. providers' confidence in consistent and clear standards, good for the edTech sector
    c. children, parents, school staff and systems administrators to build trust in safe, fair and transparent practice, so their rights are freely met through design and default

2. Schools give children's personal data to many commercial companies during a child's education. It is rarely based on consent, Article 6(1)(a) or 8(1), but assumed, "*for the performance of a task carried out in the public interest*." A code should clarify any boundaries of this legal basis where it is an obligation on parents to provide the data, and what this means for the child on reaching maturity and after education.

3. Amendment 117(2)(a) should help companies understand "*data protection by design and default"* in practice, and [child] appropriate 'significant legal effect' (Baroness Ludford, Second Reading Col 144-5). The edges of 'public interest' in Clauses 17(1)(1) (transfers to a third country) and 9(2)(g) (special categories of data), will affect children in schools.

4. Amendment 117(2)(b) and (c) help children and those with parental responsibility, understand the effect of the responsibilities of controllers and processors, for the execution / limitation of their own rights.

[1] Submission on the WP29 guidance on automated processing and children - sample case studies in England pp 3-6 http://defenddigitalme.com/wp-content/uploads/2017/12/DDM_Response-to-Working-Party-29-Guidelines-on-Automated-individual-Decision-making-and-Profiling-for-purposes-of-Regulation-2016_679_v1.2-2.pdf

5. The Article 29 WP further recommends, "*Because children represent a more vulnerable group of society, organisations should, in general, refrain from profiling them for marketing purposes.*" What will this mean for software platforms that profile users meta-data to share with third parties, or commercial apps signed-up-for in schools that offer advertisements in-use, or bait and switch premium model?[2]

6. Setting out child appropriate safeguards is necessary under GDPR Articles 13(2)(f), and 21-23 for exemptions. The Bill Schedule 1, Part 2 (5)(2) fails to set out required safeguards designed for children.

7. Definitions of *"appropriate technical and organisational measures"* and what is expected to be *"appropriate to the risk"* for children under Recital 38 (children merit special protection) and UNCRC principles are needed. Small businesses and schools need information on acceptable and necessary levels of *"pseudonymisation, encryption, and on transmission"*.

8. Joint-controllers treat the same data differently. Schools need guidance on compliance where i) processing data under instructions from the controller(s) may differ from their own need and ii) there is a potential conflict in the best interests and restriction of the fundamental freedoms of the child, with regard to mass exports of school census data, for re-use.

9. Further important rights the amendment addresses include with reference to GDPR Article 40:
(h) the measures and procedures referred to in Articles 24(3) (responsibility of the controller) and Article 25 (especially *"by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons")* as per Clause 55 (5) of the Bill, and retention periods, and measures to ensure security of processing (Article 32);
(i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;
(j) the transfer of personal data to third countries or international organisations;

10. Subject Access is restricted by Department for Education today through the Research, History and Statistics exemption (section 33(4) of the DPA), to personal data in the national pupil database (ref. PQ108573) GDPR Recital 63 states that a data subject should have the right of access to personal data, collected concerning him or her, at regular intervals, in order to be aware of and *verify the lawfulness of processing*. *(Case C-141/12)*. Will the Department ensure that children have this right under this Bill?

Limitations and definition

- Education is devolved. Compulsory education ages are different and the issue of being in compulsory education and 18 does not arise elsewhere.
- A code does not prevent guidance being provided for use elsewhere. It would however clearly be welcome if it consistent child rights as regards data were shaped to apply across the UK.
- In the Education Act 1996, "pupil" means a person for whom education is being provided at a school, other than—
    (a) a person who has attained the age of 19 for whom further education is being provided, or
    (b) a person for whom part-time education suitable to the requirements of persons of any age over compulsory school age is being provided.

With the meaning "pupil" ICO can recommend and consider capacity appropriate standards not only on age, but in the best interests of every pupil, within the meaning of the 1996 Education Act[3]. Beyond this, there are also pupils in education, for whom parental responsibilities and oversight of consent can continue up to age 25 with SEND and an ECH plan in education, but for whom the Bill makes no provision beyond age 18. While SEND legislation takes account of this, this Bill without mention of capacity rather than age, does not.

Trust and confidence

Without guidance there is unlikely to be improvement on today's practices. Schools today have a lack of confidence using edTech from suppliers, have poor practices, and fail to inform parents/children of their rights.

US-based education platform Edmodo confirmed 77 million account details were stolen this summer – more than 2 million of them in the UK – across 550,000 schools worldwide. Can a pupil or parent object to using an app for maths homework, parent-school communications, or sickness reporting? Does an obligation to deliver education include any software use is compulsory, rather than the aim behind it?

[2] Class Dojo poses Data protection Concerns for Parents (2017) Williamson, B. and Rutherford, A. http://blogs.lse.ac.uk/parenting4digitalfuture/2017/01/04/classdojo-poses-data-protection-concerns-for-parents/
[3] The Education Act (1996) meaning of "pupil" http://www.legislation.gov.uk/ukpga/1996/56/section/3

DfE has a self-certification scheme for cloud providers. Despite recognising that children may not be competent without parental involvement, "t*here are obvious difficulties with schools deciding if children are competent enough to understand any explanation of their data being used for advertising, and to understand and exercise their right to object, without parental involvement.*" there is no guidance that this should be done, or similar comprehensive statutory guidance on personal data collected from a child using classroom apps, AI, bodycams, CCTV and IPTV. Cloud providers are not barred from enabling targeted marketing and advertisements.

Most parents do not know the school sends their child's named record to the DfE each term. Our research in 2015-16 showed only 1% awareness. The nationality collection that began in October 2016, started to change this, and 2.2% pupils have actively refused recorded, plus over 25% for whom it is not yet obtained.

Self-certification fails. Q 3.4 of the DfE model asks whether services ensure that schools are able to comply with their obligations with regard to the exercise of data subjects' rights. A leading school information management software replies yes. But their system does not offer any subject access reports that can be extracted or printed to tell a pupil or parent to whom which of their data were given, for what purpose or how long. Once data have left school systems and are sent to the DfE in the termly school census, the DfE cannot tell schools to whom they have given a child's named or identifiable record from the National Pupil Database, -- which now holds the personal confidential data of over 23 million people without their knowledge or consent -- answer to 109113 they do not know how many children's identifying data they have given away since 2012 because, "*The Department does not maintain records of the number of children included in historic data extracts.*"[4]

Where personal data from children and pupils are distributed in the education sector

Schools commonly demand the use of apps online services, or "information society services" by default. Teachers and administrators create accounts for children for classroom apps with varying degrees of personal data collection, cashless payment apps, sickness reporting or classroom platforms; Google Education or Microsoft.[5]

The commercial digital market in England's schools is vast and hard to get a good overview[6].
There is no body that has oversight of this, or that vets apps or the introduction of Internet connected objects (IoT)[7] in the classroom. Teacher training lack any standard content on child rights, data protection and privacy.

At local level: Commercial products are everyday in schools and education bodies are increasingly buying AI, even to create seating plans based on children's behavioural profile marketed as ways of reducing workload through reduced administrative time. The resulting rapid transfers of pupil data at scale to commercial third parties, have no oversight. Children need an independent data guardian.

Data can be sent abroad: Some schools use apps based in Australia to process children's absence.
These data include sensitive health data and even SEN data (autism, learning difficulty, hearing and visual impairment, mental health, emotional needs, disability.) Platforms and apps are also US based.

Biometric data are collected in library, print, locker and canteen service use based on fingerprints, iris scanning, palm prints and using RFID, profile children's behaviours in extreme detail. There is no obligation today to explicitly register biometric or children's data at categories of processing with the Information Commissioner, despite its everyday adoption in schools and the associated automated profiling. This would be welcomed.

At national level: Children's personal confidential school records are handed out to companies to turn into products and knowledge they sell. Our children's personal data from their school records have been commoditized without consent, and they are offered no right to object. The Department for Education relies on the organisation not *publishing* the pupil-level data, but hands out pupil data without small numbers suppression.

[4] http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2017-10-23/109113/
[5] Letter of the Chair of the Article 29 Working Party to Microsoft (15.02.2017)
[6] defenddigitalme is mapping the digital landscape in England's schools for a report to be published in Spring on data privacy and protection
[7] The Blackett Review (2014)

The National Pupil Database in England is the least confidential

- Only in England are children's personal confidential school records distributed at pupil level to commercial companies and other third parties since 2012 as raw identifying data, without small number suppression, from the National Pupil Database, after the Education (Individual Pupil Information) (Prescribed Persons) (England) (Amendment) Regulations 2010 and The Education (Individual Pupil Information) (Prescribed Persons) (England) Regulations 2013
- In Scotland the government national level dataset doesn't include pupil names.[8]
- In Northern Ireland it is similar, but with small number suppression[9], so it is less identifying.
- In Wales researchers[10] have access, but the English regulations do not apply that broadened the prescribed persons to journalists, data consultancies, think tanks, and other third parties.

Data released to over 1,000 third parties since March 2012 have not been anonymous, but identifying when given away for commercial re-use to a wide range of third party data users. Highly sensitive information are given away including reasons for permanent school exclusions such as sex, alcohol, theft, and violence. Indicators for services' children and adopted-from-care are also handed out.

From January 18, pregnancy, mental and further physical health data will be recorded on the national named records for and distributed to third parties in the same way as today, following SI 807/2017. Over twenty child rights advocates have written to the Secretary of State for Education, with concerns that collecting these named records, and distributing confidential data[11] will put some of our most vulnerable children at new risks. Young Offender data will be collected on a named Alternative Provision school census record from January 18, 2018 and will be retained and distributed forever, without any end date. Unlike criminal records which can be filtered from distribution or expunged under the Rehabilitation of Offenders Act 1974.

There has never been a privacy impact assessment or human rights assessment of the national pupil data collections since the database began in 1996 or with each Statutory Instrument since [HL2783].[12] The Department refuses to do so, and says the new collection poses no additional risk to privacy.

In Committee on November 22, Lord Stevenson spoke about the risks that even anonymised datasets pose children, saying, *"we should look at this again.[...] others may want to speak to the risk that it poses also to children, in particular." [Col 210]* By contrast, these data releases are **identifying**. And what a risk.

In answer to PQ109113 the Department confirmed they do not know how many children's identifying data they have given away in each of over 1,000 identifying releases since 2012, since, "*The Department does not maintain records of the number of children included in historic data extracts*."

Lord Hyde said that "*the Government are fully committed to the cause"*, of improving online safety".Should we not expect an equal commitment to how the state handles our children's sensitive data?

The Minister of State for Home Office, Baroness Williams of Trafford noted on October 10, *"the Communications Committee noted with approval the enhanced rights that the GDPR would confer on children, including the right to be forgotten, and asked for those rights to be enshrined in UK law as a minimum standard."* This does not apply to children's data collected in education. The National Pupil Database is retained and distributed forever.

Not all 'research' are equal. We recommend that amendments seeking to reframe definitions of research, or weaken oversight of who and how access to sensitive data is granted, are not snuck in at the eleventh hour, after informed discussion in shaping the GDPR. The "Framework for Processing Data by Government" appears[13] to create new powers to copy paste a similar disregard for rights at the DfE, across all administrative datasets.

---

[8] FOI request to Scottish government https://www.whatdotheyknow.com/request/pupil_data_scotland_national_dat_2#incoming-1005066

[9] FOI request to DENI https://www.whatdotheyknow.com/request/pupil_data_n_ireland_the_nationa_2#incoming-1002204

[10] Wales PLASC http://www.adls.ac.uk/welsh-government/welsh-pupil-level-annual-schools-census-and-pupil-attainment-dataset/?detail

[11] According to analysis by children's data privacy group defenddigitalme, 86% of the releases were of individual level, identifiable and sensitive or highly sensitive data. The DfE relies on the user not *publishing* the pupil-level data, but hands it out without hiding small numbers. This year only one release of data from between Jan 2017 and May 2017 was not at pupil level.

[12] A list of laws that require the collection of pupil data including Statutory Instruments in the Annex attached to the answer to HL2783

[13] medConfidential https://medconfidential.org/wp-content/uploads/2017/12/medconfidential-Data-Protection-Bill-175-178.pdf

Children's Rights

The Council of Europe 2016-21 Strategy on the Rights of the Child,[14] has an entire section on the digital world. It makes clear that, *"Children have the right to be heard and participate in decisions affecting them"* and recognises that capacity matters, ***"in accordance with their age and maturity"***.In particular attention should be *"paid to empowering children in vulnerable situations,* ***such as children with disabilities.****"*

It recognises in para 5.3. that "provision for children in the digital environment ICT and digital media have added a new dimension to childrens right to education" exposing children to new risks in, "privacy and data protection issues"[15] and that "*parents* ***and teachers*** *struggle to keep up with technological developments. "*
UNICEF's recent working paper on children *Privacy, Protection of Personal Information and Reputation says*, "*it becomes evident that* ***children's privacy differs both in scope and application from adults' privacy.*****"**

UNCRC demands policy makers aim to ensure every child is safe, has effective access to and receives education, services, and recreation opportunities - to develop **to their fullest potential.** Article 12 of the Convention on the Rights of the Child (the Convention) a right to be heard, is a unique provision in a human rights treaty; it addresses the legal and social status of children, who, on the one hand lack the full autonomy of adults but, on the other, are subjects of rights. It is vital to balance the rights of safety, privacy, and participation.

Participation of young people themselves has not been encouraged in the Bill development. The needs of young people has predominantly focussed so far, on Internet safety, but participation and privacy need taken into account as well, and the views of young people, as outlined in outputs from workshops in academic-led projects such as in *The Internet on our Own Terms: How children and young people deliberated about their digital rights.*[16]

In 2010, the Committee of Ministers adopted Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling, and made special reference to the harms of solely automated decision making and profiling, and recommended they were barred for children:

"The use of profiles, even legitimately, without precautions and specific safeguards, could severely damage human dignity, as well as other fundamental rights and freedoms, including economic and social rights.

In the UK this has not happened, so if solely automated decision making and profiling should not routinely concern a child, to respect Recital 71 of GDPR, and the CoE Principle 3.5, "*profiling of persons who cannot freely express their consent be forbidden, especially, for example, adults with incapacity and children, within the meaning of the UNCRC,"* there must be change in policy, in practice and strong codes for effective enforcement. Our children's future is being shaped by data, and through this legislation, by their safeguards or lack thereof.

Jen Persson

jen@defenddigitalme.com
m: 07510 889833
w: http://defenddigitalme.com
Twitter @defenddigitalme / @TheABB

About defenddigitalme and what we do

We are a non partisan civil society organisation. We campaign for safe, transparent and fair use of personal confidential data across the education sector in England. We received our first funding in the form of a single annual grant from the Joseph Rowntree reform Trust Ltd in April.

[14] Council of Europe Strategy for the Rights of the Child 2016-21 Para 37, p15/36 https://rm.coe.int/168066cff8
[15] Ibid. p10/26 (6) Para 21. And 28 EU Kids Online (2014), EU Kids Online: findings, methods, recommendations
[16] The Internet on our Own Terms: How children and young people deliberated about their digital rights.(2017) Coleman, S., Pothong, K., Vallejos, E.P and Koene, A. (University of Nottingham, Horizon Digital Economy Research, 5Rights)