defenddigitalme Data Protection Bill Briefing

Contents

1. Table of suggested amendments and clarifications 2
2. Background: case studies on children and profiling 7
3. Background: pupil data used in commercial research 8
4. National pupil data use by ‘for-profit’ companies 9
5. National pupil data access by journalists 9
6. Future thinking 10

Summary of topics and clauses addressed

	Topic	UK Bill	GDPR
1	Age verification	8 (Plus explanatory notes mentions “Part 3 of the bill”)	8 (2)
2	Children and a right to erasure	Clause 98 in the section Part 4 (Chapter 3) Intelligence services	17(1)(f) and 17(3)(b) and (d)
3	Data subject's rights to representation	173	80
4	Children merit specific protection and right to opportunity to give consent only to certain areas of research.	Schedule 2 Part 6 25 (2)(c) and (d)	Recitals 33, and 38 Exemptions Article 6(4); Recital 50
5	Rights to object to automated profiling	Clause 13 Clause 47	Recital 71 Article 22
6	Immigration exemption	Schedule 2 Part 1 (4)	Recital 14
7	Public interest exemption	Schedule 1 part 2 6(1) and 6(2)(d) 8(1)(c)	-
8	Power to make further exemptions	15	-
9	Data subject's rights to exam scripts	Schedule 2, Part 4 (23)	-
10	Appropriate policy documents	Part 3 Chapter 2 33(4)(b) and 40(1)	-
11	Economic well-being: other exemptions	Schedule 11 Other exemptions Part 4 (8)	-
12	Conditions for processing: Data already published by the data subject	Schedule 10 Conditions for sensitive processing (4)	-
13	Journalistic exemptions	Schedule 2 Part 5 exemptions based on 85(2) Clause 24 8(a)(iv) and with reference to 24(9) and (24(5)	-

1. Table of suggested amendments and clarifications

	Topic	Recommendation	UK Bill	GDPR	Comment
1	Age verification	Clarification why this is missing in Chapter 2. If it applies regardless from GDPR without appearing on face of the UK Bill, then amendment may be needed to ensure goal of 8(2) age verification does not mean additional personal data are collected	Part 2, Chapter 2 (8)	8 (2)	This needs clarification why this has this not been transposed in Chapter 2(8) as it is not a matter for derogation but has been mentioned in the EN for Part 3: “Part 3 of the Bill does not transpose Art 8(2) on the basis that is a matter for relevant statute or case law regulating processing to specify the objectives of processing, the personal data to be processed and the purpose of the processing," says the Explanatory Notes (p98/112). GDPR Article 8(2) presents a risk that personal data are collected that would not otherwise have been necessary, essentially exploiting age verification to capture valuable data on familial relationships. If this becomes standard practice, this legislation will be harmful not helpful to children’s privacy. Verification not data capture must be the goal, to provide the website with a single attribute of confirmation. “Such services should follow the EU’s eIDAS Regulation and the UK’s GOV.UK Identity Assurance standards, i.e. reusing credentials that already exist.” The UK has set the requirements for age verification to 13. This does NOT enable children from age 13 to consent to the gathering of personal data by companies but allows them to proceed without a holder of parental responsibility approval. This article 8 does not give children or parents new rights or base age of consent on evidence or capacity. It creates a responsibility for providers of ‘information society services’ (excluding counselling services) to ask for age verification if their services target a child, and if under 13, the provider must ask for approval from the holder of parental responsibility before collecting the child’s personal data in use of its services.

2	Children and a right to erasure	Addition to DP Bill to explicitly transpose Article 17 on the face of the bill Make an addition. The right to erasure should be automatic to offer specific protection for children where the data refer to reasons for exclusion from education. The timing for erasure and restriction of processing (filtering from disclosure) should be in accordance with at minimum the (spent and filtered) time periods the Rehabilitation of Offenders Act 1974.	This is only explicit in Clause 98 in the section Part 4 (Chapter 3) Intelligence services	17(1)(f) and 17(3)(b) and (d)	The UK has not drafted the universally applicable article 17 explicitly on the face of the bill, which seems remiss given its prominence in the Queen's Speech, although a specific right-to-erasure *from social media platforms at 18 or above*, is somewhat of a fiction, as it is not in GDPR. GDPR 17(1)(f) does make explicit mention of data collected by online information society services (not ONLY social media companies) as a child. The permitted derogations allowed are broad under GDPR 17(3)(b) and (d). The GDPR however makes no differentiation between company and State. The GDPR recitals 65, 66, 68 and 69 make clear a right to erasure has no age limits, upper or lower. However, in reality children often find their data managed by the state are subject to research exemptions, meaning the right to erasure is often overridden. Children today have no way to have reasons for exclusion from education with similar properties as criminal offences (assault, drugs, sexual misconduct, theft) erased or restricted from processing throughout their lifetime, as an example. These labels are permanent in the national pupil database, and are used in research, as well as for direct interventions in the Troubled Families Programme, and National Citizen Service. These data are also given to third parties including journalists, but are never deleted.
3	Data subject's rights to representation	Transpose GDPR article 80(2)	173	80	"Paragraph 53 omits from Article 80, representation of data subjects, where provided for by Member State law" from paragraph 1 and paragraph 2," [Data Protection Bill Explanatory notes, paragraph 681 p84/112]. 80(2) provides for NGOs to take action independently on behalf of people that may have been affected by a data protection infringement without a named individual to represent.This should be transposed so that children and vulnerable groups' data rights can be empowered with meaningful action behind it, to promote better practice. Especially important for vulnerable groups, and those potentially unaware of their rights, such as children.

4	Children merit specific protection and right to opportunity to give their consent only to certain areas of research.	Addition to ensure the spirit of empowerment of child rights in the GDPR are possible to enact in practice through the UK Bill not restricted through exemptions Add: 25 (3) (c) by virtue of recital 33 data subjects are given the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.	Schedule 2 Part 6 25 (2)(c) and (d)	Recitals offer children rights: 33, 38 Exemptions Article 6(4); Recital 50	GDPR Recital 33 says that “data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.” We would very much like to see the “specific protections” merited by children in GDPR Recital 38 including those rights to nuanced consent of GDPR Recital 33, applied to children for use of their data including in research, and not overridden, as exemptions scattered in the UK Bill seek to do. The Explanatory Notes (p15/112) state that, further, "the Bill contains provision to exercise derogations so that research organisations do not have to comply with an individual’s rights to rectify, restrict further processing and object to processing where this would seriously impede their ability to complete their work, and providing that appropriate organisational safeguards are in place to keep the data secure. In effect, these derogations maintain the status quo.” The status quo however for children is that they are exploited for-profit without consent under 'research' uses. (See this document for background case studies after table on pages 8, 9 and 10).
5	Rights to object to automated profiling	Amendment could be made to add clause 47 (3) and 13 (1) to include the line from Recital 71 “such measures should not concern a child,” to make this explicit on the face of the bill.	Clause 13 Clause 47	Recital 71 and Article 22	The Explanatory Notes fail to include that these measures regards profiling, under GDPR recital 71, "should not involve a child" and the lengthy explanations on safeguards for fair and transparent processing in this way, listed in recital 71. (See case studies after this table on p7 how extensive profiling is in education is today without understanding by children or parents, often even staff, without rights to object or ask not to be solely subject to automated profiling without explanation, or course of redress or error correction.)

6	Immigration exemption	Removal of UK Bill clause	Schedule 2 Part 1 (4)	- Not in GDPR. The opposite, protection, is given by Recital 14	This does not exist in GDPR. Schedule 2 Part 1 (4) creates a broad new exemption, outside the scope of GDPR, for any data subject rights if "for the purposes of the maintenance of effective immigration control, or the investigation or detention of activities that would undermine the maintenance of effective immigration control". "The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data."[GDPR recital 14]
7	Public interest exemptions	Tighten this broad "substantial public interest" exemption.	Schedule 1 part 2 6(1) and 6(2)(d) 8(1)(c) Substantial public interest	-	Not in GDPR. Schedule 1 part 2 Substantial public interest 6(1) and 6(2)(d) and 'detecting unlawful acts'. Would these broad clauses be used to process population wide school or health records with no opt out? Or everyone's data for immigration enforcement? Clash with GDPR recitals 33 and 38.
8	Power to make further exemptions	Tighten this broad power.	15	-	This is not in GDPR. In addition to the children specific items attached, we think clause 15 is far too broad, and should be amended to ensure there are not open ended data exemptions added indefinitely through secondary legislation, beyond what the DPA 1998 permits today. We have seen through the expansion of the school census, adding country of birth and nationality data in 2016 intended to pass to the Home Office for immigration enforcement, denied during the introduction of the Statutory Instrument, how far reaching and harmful secondary legislation can be, if the process for scrutiny is rushed and inadequate.
9	Data subject's rights to exam scripts	Remove	Schedule 2, Part 4 (23)	-	This is not in GDPR and If this were to be made exempt as set out in the Bill, it would be a *reduction of rights* that are currently possible to act on today. The Data Protection Act gives us the right to see information held about us. [source the ICO] This means you can request information about you and your exam performance, including: • your mark; • comments written by the examiner; and • minutes of any examination appeals panels.

10	Appropriate policy documents	Amendment: Require documents to be published	Part 3 Chapter 2 33(4)(b) and 40(1)	-	This is not in GDPR. The kind of data sharing policy documents that can be harmful and used in secret have included the Memorandum of Understanding using children's pupil data for Home Office immigration enforcement. The Home Office refuses to publish transparent documents. An amendment would be positive to ensure these policy documents are published to ensure transparency, especially where they concern children at very least aligned with Recital 38, and applied only with stringent case exemptions.
11	Economic well-being: other exemptions	Remove	Schedule 11 Other exemptions Part 4 (8)	-	This is not in GDPR and is far too broad an exemption and contradicts the spirit of the GDPR and intentions to promote balance of rights and responsibilities.
12	Conditions for processing: Data already published by the data subject	Remove	Schedule 10 Conditions for sensitive processing (4)	-	This exemption suggests it would reduce a data subject rights compared with today in DPA 1998 principle 2 (broadening schedule 3), that there should be reasonable expectations of purpose limitation when someone chooses to make their personal data public in a certain context. E.g. If a teenager makes information public on social media the data are 'public' within a user community but the person does not expect they are used for other purposes. Case study Danish researchers from Aarhus University scraped and released a sensitive dataset of 70,000 subscribers personal data and sexual preferences to the online dating site OkCupid. The subjects posted their data with an expectation it is public in context, for a specified purpose, not to anyone for anything at all.
13	Journalistic exemptions	Remove or amend	Schedule 2 Part 5 exemptions based on 85(2) Clause 24 8(a)(iv) and with reference to 24(5)	-	This exemption is incompatible with GDPR Recital 38 - children merit specific protections. (See case studies in this document page 9) Further, much of today's journalism via social media platform distribution for example, is not regulated by the bodies in 24(5). This seems too broad an exemption designed for an outdated view of what the press and publishing in clause 24(9) and journalism are today.

2. Background: case studies on children and profiling

The range of ways in which children are profiled in school-wide applications using children's personal data from school records, often including photographs as well as sensitive personal data, and without consent, are not transparent to pupils and parents, or often even to school staff themselves. It is vital that the spirit of GDPR recital 38 "children merit specific protections" is carried across the provision of the UK Bill and that exemptions do not reduce rights to processing, or object to automated profiling which "should not concern a child" (recital 71).

Schools use commercial apps which use children's personal data to create profiles

- that create persistent and permanent behavioural records,
- that claim to use AI and machine learning to profile that behaviour and claim to identify how pupils influence each other in the classroom, using AI to automatically generate seating plans.
- for certain basic functions such as homework communications and tracking, or medical records field-trip management and sickness tracking, and cashless payment systems that store the parents' financial details as well as child's personal profile.
- For biometric profiles of library, print, locker and canteen service use based on fingerprints, that store children's biometric data and children's activity down to the nth degree, even down to what they buy and its nutritional content.

School-wide seamless integration with the pupil information management systems, means that children's personal data are sent to the commercial third party provider before the parent and pupil have been informed, and without any choice or ability to say no. There is no oversight or accountability for the effects of education technology providers in UK state schools, or interference with privacy. Many commercial apps are free to schools, but offer premium in-app paid services to parents and pupils, or other secondary services such as private tutoring. Parents and pupils are often not offered any opt out or choice and schools say they require use of the system and demand flawed "consent" in pupil /parent signed digital contracts. These can mean sending data abroad, exempt from data rights, or exposure to onward third-party uses.

Some schools use or propose using wearable devices, to profile activity. A school in West Cheshire profiled every movement using RFID[1]. Schools assign devices without assessment of the impacts on child mental health of constant surveillance, or the vast data lakes that they send children's data to forever. Sports researchers Drs Kerner (Brunel University London) and Goodyear (Birmingham University) recently carried out a study of teenagers and found fitness trackers and apps may not be positive health promotion tools. Wearing the device made some pupils lose confidence in their physical ability. Others said the device made them feel fat and uncomfortable with peers.Their reasons for taking part in physical activity also changed. For example, after the eight weeks, more pupils reported taking part in physical activity because they felt pressurised.

Web monitoring includes profiling through keyword logging and real-time screen recording of all internet use, both in school and at home, without transparency, on school provided laptops or software installed on personal items in bring-your-own-device. Web monitoring systems typically, "continuously build a profile of all users, allowing the system to accurately interpret between a one-off event or a consistent pattern of behaviour." It is common for school policies to make no mention of what policy there is on monitoring, keywords of third party access, and retention, error rate, or course of redress. Yet many of these companies are monitoring 24/7 every day of the year and potentially may each be affecting the lives of "half a million students and staff in the UK" without oversight or public or school awareness of their accuracy, accountability, or otherwise.

We know of children wrongly labelled as at risk of suicide or gang membership, unable to delete their records or with any course of recess for correction, and staff trapped in a risk averse system geared to protecting the school, more than the rights of the child. National policy made this type of practice standard in statutory guidance introduced in September 2016, without public consultation or scrutiny. Better policies and practice, will come through child rights on profiling.

[1] https://www.theguardian.com/technology/2013/nov/19/college-rfid-chip-tracking-pupils-invasion-privacy

3. Background: pupil data used in commercial research

There is no ability for children to effect their rights to privacy if the State decides these uses qualify as research. Therefore safeguards in GDPR recital 33 should be assured for children to opt out.

The National Pupil Database (NPD) is "one of the richest education datasets in the world" according to the DfE User Guide[2]. The NPD holds detailed personal information from every child in state education, and some independent school pupils since 1996. It now includes nearly 23 million individual named records[3]. In any given year the total is ca 8 million[4] active pupils and a new intake adds 700,000 more. The majority of NPD is collected 3x a year in the school census.

Individual level pupil data are handed out to third party recipients. These include commercial companies, websites, charities, think tanks, newspaper and TV journalists, and one-man-band data intermediaries and consultancies. (see next page for summary case studies).

David Cameron[5] announced in 2011, that the government would open up access to anonymised data. But the pupil level data released since, are *not anonymous.* Data are released in four tiers of identifying and sensitive data[6], and there is no consent for its release. There is no small numbers suppression applied to extracts before release (as confirmed via FoI about the 2013 release of identifying and sensitive pupil-level data to the Telegraph of millions of records).[7]

The sensitive and identifying items that require DMAP approval include name, date of birth, postcode, candidate numbers, Pupil Matching Reference (Non Anonymised), detailed types of disability, indicators of adoption, reasons for exclusions incl. theft, violence, sex, alcohol.[8]

Of the documented 887 third party requests for identifiable data that went through the DfE Data Management Advisory Panel (DMAP) request process between March 2012 and December 2016, only **29 were for aggregated data.** The handful of rejected applications included a request made "by mistake" from the Ministry of Defence to target its recruitment marketing[9]. About 60% of the applications approved for identifying and sensitive pupil level data, were from commercial companies, think tanks, charities and press. 40% academic. Under were refused 15 since 2012.[10]

In a presentation in Sept 2016, the Director of the DfE Data Modernisation group acknowledged the release of sensitive data: "*People are accessing sensitive data, but only to then aggregate.The access to sensitive data is a means to an end to produce the higher level findings*."[11]

---

2 NPD User Guide p 5/40 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/472700/NPD_user_guide.pdf

3 FOI https://www.whatdotheyknow.com/request/pupil_data_national_pupil_databa_2?nocache=incoming-764676#incoming-764676

4 http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2017-02-02/62925/ Schools: Census Parliamentary Written question - 62925

5 Cameron, David (July 7, 2011) https://www.gov.uk/government/news/letter-to-cabinet-ministers-on-transparency-and-open-data

6 Ref pp19-21 Tiers 1-4 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/472700/NPD_user_guide.pdf

7 *"There is no suppression applied to data extracts from the NPD before release"* http://defenddigitalme.com/wp-content/uploads/2017/05/Telegraph.pdf

8 DMAP Terms of References pages 10-14 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/537139/Data-Management-Advisory-Panel-terms-of-reference.pdf first published via FOI in 2015 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/537139/Data-Management-Advisory-Panel-terms-of-reference.pdf

9 Schools Week June 2015 http://schoolsweek.co.uk/mod-makes-inappropriate-request-by-mistake/

10 Pupils Personal Records: Parliamentary Written question - 57722 Jim Cunningham to Nick Gibb http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2016-12-14/57722/

11 Presentation to NPD User Group Sept 2016 http://www.bris.ac.uk/media-library/sites/cmpo/documents/bradley2016.pdf

4. National pupil data use by ‘for-profit’ companies

1. Case study: [**download Tutor Hunt case study .pdf 929 KB**]

A private tutor-pupil matching service Tutor Hunt, is one of the largest tuition web sites within the United Kingdom with more than a quarter of a million registered users signed up.

It is hard to see how this qualifies as ‘research purposes’ because data is used to create a website product, rather than ‘research’, namely show heat maps of pupils around each school in England.

The request for identifying data made to the Department for Education Data Management Advisory Panel in 2015, said that its purpose for getting home postcode, date of birth (month and day) plus Schools Unique Reference Number, for all pupils at all schools was, “*to give parents a quick and easy way to determine which schools they can apply for and how likely they are to attain a place at the school, and requires the post code of all the students at each school to achieve this.”*

2. Case study: [download Mime Consulting case study .pdf 818 KB]

“We use data from the NPD to track your students wherever they go within England.” Commercial data intermediaries are processing pupil data supplied by schools and from requests of the NPD, with little oversight of use after release, without pupil or parental knowledge.

5. National pupil data access by journalists

Journalists have been given pupils’ SEN data, ethnicity, language, armed services and children in care indicators, and date of birth, even though there is no clear legal basis for passing journalists data (under the Prescribed Persons Act) or meeting Schedule 3 of the Data Protection Act 1998.

1. Case study: [download BBC Newsnight case study .pdf 785 KB]
BBC Newsnight was granted Tier 1, the most highly sensitive identifying data matched with all KS2, KS4 and KS5 attainment datasets.

2. Case study: [download The Times case study .pdf 1.4MB]
Identifying, sensitive data released in to The Times, “to pick interesting cases/groups of students.”

3. Case study: [download The Telegraph case study .pdf 1.6MB]
The Telegraph newspaper[12] was granted identifying and sensitive data in 2013, for all pupils in the KS2, KS4 and KS5 cohorts for the years 2008-2012. That’s about 9 million records.

There is no small number suppression applied to data extracts from the NPD before release. Instead, “requesters are required to sign up to strict terms & conditions covering the confidentiality and handling of data, security arrangements, retention and use of the data”. These include saying that no individual will be identified in published data. *“The Daily Telegraph requested pupil-level data and so suppression was not applicable.”*[13] The DfE wrote an email after discussion of their application[14] saying the journalists were ‘not looking to compare the performance of individual teachers’ and they offered *“cast iron assurances that no children will be identified through the use of this data*”. Not that they couldn’t do it, but assurances that they wouldn’t do it.

---

[12] February 2013 identifying sensitive data release http://defenddigitalme.com/wp-content/uploads/2017/05/Telegraph.pdf

[13] FOI: no small numbers suppression https://www.whatdotheyknow.com/request/pupil_data_sensitive_data_releas#comment-69968

[14] DfE letter on assurances given by journalists at the Telegraph after their application for all data on children, and before being sent identifying data https://www.whatdotheyknow.com/request/293030/response/738135/attach/2/Annex.pdf

6. Future thinking

The GDPR has been several years in the making, so some of the thinking is already outdated. The UK Bill reflects current thinking, and does not consider the changing nature of profiling from machine learning using population wide data or facial recognition using billions of photographs in a short time-frame. As such, sensitive data protections from future uses which change beyond those expected at the time of collection, for example children's photographs, in Part 2, Schedule 1 are inadequate in the Bill. First principles to bear in mind, include that the UK has chosen to apply this regulation and DP Bill only to the living. The Bill does not apply to the personal data of deceased persons. Member States may provide in Recital 27 for rules regarding processing of personal data of the deceased. Data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information are still to be considered to be information on an identifiable natural person. [Recital 26].This must not be watered down further to enable exemptions for pseudonymised data, as it was the subject of extensive debate and lobbying during the development of the Regulation. To do so would be detrimental long term.

If research uses are to be trusted, then the consent process in which direct and indirect uses are conflated is fatally flawed and will not be legitimate under GDPR. Those who carry out research must ensure that trust is maintained by not using data in ways we do not expect. The GDPR aims to enable use of data and is not a barrier to innovation, as long as organizations implement the appropriate safeguards. The right balance must be struck.

Given the volume of sensitive data about children in the UK, including the DNA taken from millions of [living] children stored and used without consent for research, the balance today is already out of tune with reasonable expectations. There must be a different approach here, as we proposed to NHS England Public Health in 2016. NHS England has a "genomic dream" for the Generation Genome. The views of geneticists were already presented to the Education Select Committee in 2013 to propose how genomics could be used to shape education. NHS England is reported to be spending £1.5 million on a new national database for research of all child deaths. Genetic data affects relations and lives on beyond beyond death. These uses will shape our future society. To write contemporary data protection laws that give children and parents no rights by design, seems already out of date, incompatible with privacy and data protection by default of GDPR Article 25.

When those who are supposed to be protecting us, are also those who have stolen and exploited child identities, then there is something wrong in the balance of power on personal data, and the GDPR is designed to restore some of those rights to citizens.

We believe the derogation should have been used to apply GDPR to the deceased (Recital 27) given the new NHS database on dead children, DNA, and police abuse of dead children's identities, but we suspect this will remain outside the scope of the Bill.

Children will have to live with the effects of the use of their personal data by adults, by relations, and use of their own data on social media, in health and education, in and beyond their lifetime. We should be forward looking and be including rights here for all that go beyond the living, because our personal data can be stored and used in perpetuity, and affects those who we leave behind. At very least, the spirit of the GDPR and recital 38, children merit specific protections should be a guiding light in exemptions, and we should be very clear where rights are being reduced from current Data Protection principles or seek to remove or reduce those in the GDPR.

All children's data must safe, fair and transparent, and rights based, to ensure trusted use, and to "protect the full development, without discrimination, without arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation", as underpinned by the UN Convention on the Rights of the Child.[15]

[15] https://downloads.unicef.org.uk/wp-content/uploads/2010/05/UNCRC_united_nations_convention_on_the_rights_of_the_child.pdf