



Defend Digital Me

PO Box 2280

RH20 6BJ

May 17, 2024

The Secretariat to the Debt and Fraud Information Sharing Review Board

By email only: dea-data-sharing-fraud-and-debt@cabinetoffice.gov.uk

cc The ICO via icocasework@ico.org.uk

Encl. The MOU and various sample applications for data between the DfE and the DWP.

We write from Defend Digital Me with reference to the news¹ of data sharing for the purposes of fraud detection and prevention between the Department for Work and Pensions (DWP) and the Department for Education (DfE) (“the Departments”) under the DEA 2017. We understand that the board makes recommendations to the Minister for the Cabinet Office on whether proposals should be accepted for implementation accepted subject to amendments, or declined. And that all approved proposals must proceed as pilots in the first instance.

Please can the Board review and confirm whether the processes were met, and consider rejection of future data sharing on ethical as well as legislative grounds. We request supporting evidence and information, and some supplementary administrative updates.

The MOU states on page six that, “(7) DWP and DfE both are using Section 56 of the Digital Economy Act 2017 “Disclosure of Information to combat fraud against the public sector” as the legal gateway for this data share.” and on page seven that, “Under the Digital Economy Act Code of Practice all relevant documentation, including a Business Case for this data share are to be presented to the Digital Economy Act Board in June 2022”.

1. Accuracy of public Register of Information Sharing Agreements² made under the public service delivery, debt, fraud and civil registration provisions within the Digital Economy Act 2017. The register appears to show a pilot³ between the Departments dated 01-01-2023 to 13-04-2024(*). An intra departmental data-sharing arrangement⁴ obtained via FOI request was formalised (date redacted) and requests might be (but not all are) based on it.

We ask if the Board can please clarify why and if (a) there is a corresponding routine operational agreement after the pilot between the DWP and the DfE in the DEA register and (b) if the Business Case for this data share was presented to the Digital Economy Act Board in June 2022 as described in the MOU. If so, we request a copy.

¹ Schools Week <https://schoolsweek.co.uk/revealed-secret-deal-to-let-benefit-fraud-squad-snoop-on-pupil-data/>

² <https://registers.culture.gov.uk/>

³ <https://www.digital-economy-act-register.data.gov.uk/agreements/38>

⁴ The DWP-DfE MOU <https://defenddigitalme.org/wp-content/uploads/2024/05/DfE-DWP-MOU-Redacted.pdf> the only visible date (unredacted) is in the very last line 02/10/2023

2. **DEA transparency recording:** the first DWP-DfE data distribution listed in the DfE register of datasharing⁵ for such purposes shows a date of April 2018 but the pilot *in the DEA* is only listed from 2023.

Can the Review board please clarify if you have assessed the Departments' proposals to use the powers and considered whether the requirements to use the powers were met at each point in time—in 2018, or any pilot(*), and any operational agreement with a live MOU?

3. Since the Review Board “monitors the pilots and supports any decisions made on the basis of pilot outcomes”, such as implementing the data share on a wider scale, we also and **thirdly, request a copy of (i) any analyses on the effectiveness of the pilot before any routine operational policy began, and (ii) the outcomes of your consideration whether the departments' MOU and operations meet the requirements of the Code** issued by the Secretary of State under section 43 of the Digital Economy Act 2017 and by the Minister for the Cabinet Office under sections 52 and 60.

4. Firewalls between datasets and reuses? Given that other data sharing is routine and equally opaque to the data subjects, we would like to know if and what any safeguards / processes are put in place if any by your board when data is routinely shared between the same bodies for other purposes to prevent use from one dataset for the other purposes?

5. Further request for a review of lawfulness and compliance: I draw your attention to the guidance on the Code of Practice⁶ which makes comments on processing under these powers and the necessity to also comply with data protection law, “(20) *The data protection legislation requires that personal data is processed fairly and lawfully and that individuals are aware of which organisations are sharing their “personal data” and what it is being used for (the “lawfulness, fairness and transparency” principle),*” and in “(22) *The Data Protection Act 1998 set out eight principles which had to be complied with, when personal data was collected, held or otherwise processed,*” and “(23) *Article 5 of the General Data Protection Regulation sets out six principles relating to processing of personal data. Personal data shall be: (a) “processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (“purpose limitation”).*”

The principle of purpose limitation

In paragraph 12.5 of the DWP-DfE MOU the departments state that, “*The parties agree to*

⁵ <https://www.gov.uk/government/publications/dfe-external-data-shares> (tab 6: Data shares with police and criminal investigation authorities) “A request was received from DWP involving 185 child identities to be checked against the NPD. **Of the 185 child identities**, we were able to positively match one and confirmed this to DWP as a ‘Y’ only. No individual data was shared back to DWP. DWP has extensive statutory and common law functions to a) investigate benefit fraud b) impose penalties or refer for prosecution in respect of suspected benefit fraud.”

⁶ Section 1.3 Information sharing and the law <https://www.gov.uk/government/publications/digital-economy-act-2017-part-5-codes-of-practice/code-of-practice-for-public-authorities-disclosing-information-under-chapters-1-3-and-4-public-service-delivery-debt-and-fraud-of-part-5-of-the-di>

only handle personal data **in ways that people would reasonably expect** and not use it in ways that have unjustified adverse effects on them.” However, if the outcry on social media is not evidence enough, we commissioned a poll of parents in 2018. No family reasonably expects that their own or their children’s personal confidential data are used for any national DWP process when they provide it to a school. In fact, most don’t even expect it to be passed on to the Department for Education at all.⁷ 69% said they had not been informed (ever or at the point of collection) that the DfE may give out data from the National Pupil Database to third parties. And the millions of people already in this database long before this policy began, could have no way to expect it even if schools *had* been informed in their role providing the information to the DfE in the first place, as joint data controllers.

The data protection principle of purpose limitation means **people do not expect such incompatible reuses to further other aims**, completely outside education beyond the scope of the purposes of the Education Act 1996 s 537a at the point of collection, especially by any non-DfE bodies even if they’d heard of the database, and certainly not that the DfE can simply ‘move the goalposts’ years later after the point of collection for such incompatible purposes beyond their reasonable expectations and for purposes incompatible with education and the wellbeing of children as stated in the legal gateway enabling collection.

The principles of necessity, proportionality and data minimisation

The DfE holds at least 28 million records if not more, as it constantly grows and its database sizes are not published anywhere. All of these records could be in scope for searching, including yours, and almost none of them are necessary or proportionate to search for matches against as the hay in which the search is for a fraudulent needle, yet the MOU claims in paragraph 15 to respect, “*the application of the data minimisation principle*”.

The principle of fair processing: to be informed of processing and of data subject rights

The MOU makes claims that the Departments respect the law on the Right to be Informed (Article 12, 13, 14) in the table on page 13 of the MOU states, “Existing DWP and DfE notifications are adequate”.

We point out that this is untrue. It is not what the ICO found in 2019, or when its 2020 audit⁸ declared explicitly, “[The DfE are not providing sufficient privacy information to data subjects as required by Articles 12, 13 and 14 of the GDPR](#),” and, “The DfE are reliant on third parties to provide privacy information on their behalf however, this often results in insufficient information being provided and in some cases none at all which means that the DfE are not fulfilling the first principle of the GDPR, outlined in Article 5(1)(a), that data shall be processed lawfully, fairly and in a transparent manner.”

That has not meaningfully changed in 5 years since the finding. [That obligation](#) on transparently processing everyone’s data all of the time, is not about tipping off individuals in

⁷ Survey poll of 1,0004 parents of school age children in 2018 <https://defenddigitalme.org/2018/03/13/only-half-of-parents-think-they-have-enough-control-of-their-childs-digital-footprint-in-school/>

⁸ <https://defenddigitalme.org/wp-content/uploads/2021/10/department-for-education-audit-executive-summary-marked-up-by-DDM-Jan-2021.pdf>

particular cases. The DfE has [done nothing to meet its fair processing duties](#) and shows no political will to fix it. More than 8 million children attend state educational settings every day and have no idea they have rights in relation to the national processing of their personal records, or how to exercise them since there is no clear route to do so. Families interact with schools, not national government departments. Those millions who have already left school and all educational settings, but will remain named in the database until they reach 66 years of age have no contact with their school at all. How will the departments reach them in order to fair process as well as offer those individuals their full range of human rights in relation to the processing.

The vast majority should never be under any scrutiny ever for a potential DWP match. Under what basis is are necessity and proportionality met for each person who is not in the scope of the match and yet whose data will be processed to find a no-match anyway. In effect the vast majority of each processing for this purpose is a trawler-scale fishing exercise processing millions of records in order to possibly find a match.

We ask either that these questions are resolved, or acknowledge that the information sharing is in fact without informed processing, and furthermore is neither necessary nor proportionate in the vast majority of processing and resolve these infringements of DP law.

Further Review Board administrative questions

Minutes:

We are unable to find any minutes beyond June 2021 on the website from the Debt and Fraud Information Sharing Review Board that we understand will meet monthly, except in instances where there is no business to discuss. I therefore ask for a copy of the minutes since June 2021 and also that they be published on the appropriate website.

Detail in the Register:

We also point out that there are obligations in the Code for the register to be understandable. The retention period is coded e.g. P24M and this has no meaning outside the database so we ask that the register has a regular date added or instead of, such a code.

We ask that this letter be distributed to all members of the board.

Thank you for your consideration.

Sincerely,

Jen Persson

Director, Defend Digital Me

Jen@defenddigitalme.org

m: +44 (0)7510 889833

w: <http://defenddigitalme.org/> | twitter @defenddigitalme / @TheABB

Defend Digital Me 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.