

October 29, 2017

Constitutional and Legislative Affairs Committee
National Assembly for Wales

Dear Chairman, and Honourable Members of the Committee,
separately from our recent correspondence on SI 2017 No. 940 (W. 233) we ask you to address

SI No. 886 The Education (Student Information) (Wales) Regulations 2017 (W. 214)¹

These regulations made on September 7, were laid before the National Assembly For Wales on 11 September and came into force on October 6. They enable the extraction of student confidential data and its onwards sharing with third parties, without consent.

Data affected include (a) surname; (b) each first name; (c) gender; (d) date of birth; (e) ethnic group; (f) home address and postcode; (g) the unique learner number allocated to an individual, plus further extensive detail on the relevant qualifications or regulated qualifications.

This extremely short time period is we suggest, unsuitable to create a national database, of named sensitive data for indefinite retention and third party sharing on the basis of a Statutory Instrument.

The public consultation² was conflated with another on use of destinations data, and its is not clear that this Regulation permits *identifiable* individual level data sharing, not sharing of anonymous statistics. That it had only 10 responses shows that its significance was entirely overlooked, and missed by organisations such as ourselves interested in civil liberties and child rights.

The assessment makes an utterly inadequate assessment of the sensitivity of linkage of longitudinal data from a lifetime of education with DWP and HMRC records - use for which the individual has not given consent and will not be asked. There are far reaching implications for privacy and ethics and discriminatory outcomes affecting individuals and groups.

We believe the assessment of child rights is flawed. It concludes, "We have not identified any potential adverse impacts on young people." But there is not a single mention of lifetime privacy impact. Step 3 in the assessment concludes that it does "not directly relate with the UNHRC".

Article 16 of the UN Convention on the Rights of the Child is overlooked: "*No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.*" *And the voice of young people has not been considered, an Article 12 requirement of the UNCRC.*

This is also incompatible with recital 38 of the GDPR that children's data merit special protections.

The EU Charter of Fundamental Rights [34] , Article 52 also protects the rights of individuals about data and privacy and Article 52 protects the essence of these freedoms.

The third parties listed who will get given access to the data without consent and without a right to refuse, include the Student Loans Company and "*persons who, for the purpose of promoting the education or well-being of students in Wales, require the information for that purpose*".

That near-identical wording was used in 2012 to change the law in England. Our children's privacy has been outsourced to third parties ever since. Not anonymised data, but identifiable and confidential pupil-level data is handed out to commercial companies, charities and press.

¹ SI 886 <http://www.legislation.gov.uk/wsi/2017/886/contents/made>

² Impact Assessment https://consultations.gov.wales/sites/default/files/consultation_doc_files/170901-childrens-rights-impact-assessment-en.pdf

It appears that there are no limitations on commercial companies accessing these data on the face of the SI if they “require student information for that purpose”.

The open ended list of third party sharing in Schedule 2 Part 2 and identifiable and sensitivity of personal data involved, means the purposes of data sharing in this regulation are fundamentally incompatible with Article 8, the right to privacy in the Human Rights Act 1998³ when their data will be passed to third parties beyond their control and interfere with their private life.

We are concerned that the effect of the Digital Economy Act 2017, Part 5 is the removal of horizontal data protections across government and once personal data are under the powers of the Secretary of State, data may be passed to other government departments and public bodies.

We ask you to consider that in 2015 37,000 students responded to UCAS’ Applicant Data Survey⁴. Sixty-two per cent of applicants think sharing their personal data for research is a good thing, and 64% see personal benefits in data sharing. But over 90% of applicants say they should be asked first, regardless of whether their data is to be used for research, or other things. See page 3 Annex.

Young people do not want or find it reasonable that their personal confidential data is used, particularly on an identifiable basis, beyond their control. This piece of legislation builds-in failure of public trust in data handling by design by ignoring the right to privacy.

It’s not in young people’s best interests to be made more digitally disempowered and lose control over their digital identity. The GDPR requires data privacy by design. This approach is unsuitable.

Suggestions and Questions:

1. Confirm if a privacy impact assessment (a government mandatory minimum measure since 2008),⁵ was done and when it might be published. Revisit the consultation conclusion if not.
2. Publish the assessment of the impact on fundamental human rights with regards to privacy, the European Convention on Human Rights and the Human Rights Act 1998, and UNCRC.
3. How will students be told and will the SI principles of Data Protection law of fair processing and communicating purposes, data minimisation and retention be met? The SI has no limitations.
4. Will there be a published third-party register⁶ which and why organisations access this data?
5. Is there any independent oversight of the decision making process for data access approvals and scope creep of these uses?
6. The Statutory Instrument should have considered wording on safeguards, oversight, rights to subject access, rectification and erasure, and right to objection or broad compatibility with GDPR. There is no connection made with the potential impact this will have on individuals as the effect of policy using destinations data, or to ensure policy is based on accurate data. If these issues are too late to consider in the SI, a published Code of Practice may be of merit.

Thank you for your consideration.

Sincerely,

Jen Persson

Director, defenddigitalme

³ http://www.legislation.gov.uk/ukpga/1998/42/pdfs/ukpga_19980042_en.pdf

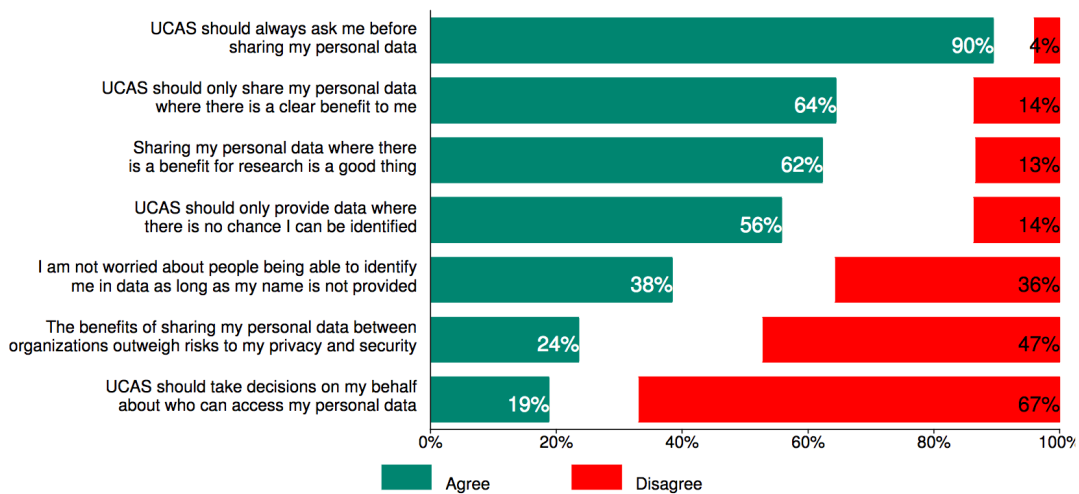
⁴ 37,000 students respond to UCAS’ Applicant Data Survey <https://www.ucas.com/corporate/news-and-key-documents/news/37000-students-respond-ucas%E2%80%99-applicant-data-survey>

⁵ See Cabinet Office, Cross Government Actions: Mandatory Minimum Measures, 2008. Section I, 4.4: All departments must “conduct privacy impact assessments so that they can be considered as part of the information risk aspects of Gateway Reviews”.

⁶ A third party use of pupil data in England is published <https://www.gov.uk/government/publications/national-pupil-database-requests-received>

Annex: Extracts from the UCAS survey to which 37,000 students responded in 2015⁷

Figure 2 Proportion of respondents (weighted) who agree or disagree with various general statements about the use of their personal data.



The responses from applicants showed a preference for remaining in direct control of their personal data. The large majority of applicants (90 per cent) agreed with the statement that they should be asked before their personal data was provided, over twenty times more than disagreed with that statement (4 per cent).

Three scenarios were presented. In each case a substantial proportion (between 40 per cent and 78 per cent) said they would trust UCAS less with their data, or would consider not using UCAS to apply to higher education, if their data were provided without their consent. For the scenario of personal data being provided to Government to speed up an application for a student loan, 60 per cent of applicants said they would be content with the arrangement, 34 per cent said they would continue to use UCAS but would trust UCAS less, and an additional 6 per cent said they would consider not using UCAS if their data were used in that way.

When asked to consider that their personal data was provided to Government and other organisations for statistical research purposes, 44 per cent said they would be content, 48 per cent said that they would continue to use UCAS but would trust it less, and an additional 8 per cent said they would consider not using UCAS.

⁷ Survey of 2015 cycle UCAS applicants on the use of their personal data <https://www.ucas.com/file/36556/download?token=lvGg2GQe>