



CHILDREN’S WELLBEING AND SCHOOLS BILL: ORG ANALYSIS OF AMENDMENT 38 B

Author: Mariano delli Santi – mariano@openrightsgroup.org

March 2026

IN THIS BRIEFING

0. SUMMARY.....	2
1. The scope of this amendment is unclear.....	3
2. This power allows the Secretary of State to override ECHR proportionality for age verification purposes.....	3
3. This power confers excessive discretion to change UK data protection law, which potentially threatens the free flow of data to and from the EU.....	4
4. CONCLUSION AND RECOMMENDATIONS.....	6

Published under a Creative Commons Attribution-ShareAlike 4.0 Unported Licence
<https://creativecommons.org/licenses/by-sa/4.0/> except where stated.

Open Rights is a non-profit company limited by Guarantee, registered in England and Wales no. 05581537.

O. SUMMARY

Amendment 38 b would introduce a new power for the Secretary of State, enshrined in new Article 8ZA, to make provisions that a data subject who has given consent for the provision of an information society service is at least of the age specified by Article 8(1) of the UK GDPR. Currently, this age is set at 13 years old.

To this end, the Secretary of State would also have the power

- To make "*provision imposing requirements on*" an information society service (ISS), including "*provision about the steps that must or may be taken by [the ISS provider] for the purposes of complying with*" such age requirements.
- To "*make provision amending, repealing, revoking or applying (with or without modifications) any provision of the data protection legislation (within the meaning given by section 3(9) of the Data Protection Act 2018)*".

Open Rights Group urges the House of Lords to reject this amendment. Alternatively, we urge the House to support Amendment (e) – Proportionality Requirement for Regulations under sections 214A and Article 8ZA, as proposed by Liberty in their briefing.

As we explain in this briefing, amendment 38 b:

- Lacks a clear, and perhaps a useful, scope. UK data protection law already requires providers of ISS to verify the age of users to determine the validity of their consent.
- Would allow the Secretary of State to mandate age verification tools that violate the privacy of children and users whose age is verified. There is no clear rationale for granting, nor is desirable to give, discretion to the government to mandate the use of unsafe age assurance tools.
- Gives the Secretary of State an overly broad power to change any provision in UK data protection law. Providing such a broad discretion for the purpose of verifying users' age is irrational, and introduces an unnecessary risk of jeopardising UK adequacy and the free flow of data with the EU.

1. The scope of this amendment is unclear

Article 8 of the UK GDPR already requires that information society service (ISS) providers must verify that users who have given consent are above the age specified by article 8(1), or by a person who holds parental responsibility over the child. Taken at face value, the regulations made under new Article 8ZA(1) would only remove parental authority to provide consent on behalf of the child. The rationale for this change is not stated.

2. This power allows the Secretary of State to override ECHR proportionality for age verification purposes.

According to Article 8(1) of the UK GDPR, information society service (ISS) providers must take “reasonable steps” to verify that a user is old enough to provide consent. Reasonableness is anchored to the necessity and proportionality tests under the UK GDPR and the European Convention of Human Rights. Reasonableness ensures that the right to privacy and data protection of a child (or an adult users) going to age verification is not violated or disproportionately affected in the process.

In practice, what is “reasonable” to verify a user age under Article 8(1) of the UK GDPR is determined by a balancing act between the risk of data processing for which a user is consenting, and, on the other hand, the risk of data processing for age verification purposes, the state of the art of the technology, the effectiveness of the age verification method, the existence of a less invasive mean to achieve the same goal, etc. This balance is currently determined by the Information Commissioners’ Office, via regulatory guidance. Such determinations can be scrutinised and overridden by UK Courts.

The power introduced by amendment 38 b would allow the Secretary of State (SoS) to mandate what age verification methods or procedures must be taken in order to comply with regulations issued via its new rule-making power. This power gives the SoS ample discretion to override proportionality considerations, as choices made by regulation could mandate age verification methods that violate or have a disproportionate impact on the privacy of ISS users.

Furthermore, this power would allow the government to use and designate a digital identity as a mandatory mean to verify users’ age. It appears inappropriate to enact legislation in this regard before the ongoing government consultation is done. Either way, allowing government rule-making to disregard proportionality criteria under ECHR would be even more concerning in a circumstance as such.

It is not desirable to give the SoS powers to mandate age verification methods that violate the privacy of children and adults, and the government has not explained why it seeks such power. Likewise, the case for allowing the government to override, without meaningful parliamentary scrutiny, determinations made by independent regulatory authorities, has not been made. There is clear value in leaving the choice of what age verification methods and tools are best to an expert regulator subject to judicial oversight, rather than to the whims of the government of the day.

3. This power confers excessive discretion to change UK data protection law, which potentially threatens the free flow of data to and from the EU.

The UK enjoys adequacy status under EU law. This is the result of a determination, made by the European Commission, that the UK provides an adequate level of protection to personal data compared to the EU. Thus, data can be transferred between the EU and the UK without additional safeguards or hindrance. Maintaining adequacy status is considered fundamental to protect the UK economy and for EU-UK relationships.

Amendment 38 b provides a power for the Secretary of State to amend, repeal, revoke or apply any provision of the UK GDPR or the Data Protection Act. The government would be given this authority without any significant condition or restriction to their discretion, beyond such power having to be exercised for age verification purposes. This power would also allow the government to amend foundational elements of data protection law, including data protection principles, data subjects' rights, or international data transfers provisions.

Giving the government such an unconditional blank cheque appears inappropriate. The breadth of such power is also unjustified. It is not clear what age verification purposes would benefit from the government power to change foundational elements of UK data protection law. The government has also not explained why changes with such relevance should be made with Statutory Instruments, thus bypassing substantive parliamentary scrutiny.

The Data Use and Access Act has already given wide discretion to the government to change UK data protection law via rule-making powers. Such powers have been identified, in the UK adequacy decision, as a major factor that could affect the level of protection afforded to data transferred to the UK. To address these concerns, the UK adequacy decision clarifies that "special attention should be paid to such additional specifications" introduced by the SoS via rule-making power.¹ The

¹ See Paragraph 120 of COMMISSION IMPLEMENTING DECISION of 19.12.2025 amending Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU)

adequacy decision also provides an unprecedented mechanism whereby the Commission could, in reaction to the use of such powers by the UK government, formally require UK authorities to introduce changes to UK data protection law within a three months period, or else proceed to repeal, suspend or amend the adequacy decision.

The introduction of a new, almost boundless mandate for the Secretary of State to amend any data protection provision is an pre-announced car crash. It introduces the substantial risk that poorly thought out changes introduced by Statutory Instruments could inadvertently jeopardise UK adequacy. Introducing such a risk appears inconsiderate, and ultimately unnecessary, for the purpose of pursuing age verification policies.

2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom (notified under document C(2021)4800), at:
https://commission.europa.eu/document/download/a7907f8f-6e1c-4782-a193-d16b2cfe7650_en?filename=JUST_template_comingsoon_standard_26.pdf

4. CONCLUSION AND RECOMMENDATIONS

Amendment 38 b would grant the UK Secretary of State new powers under Article 8ZA to introduce new age verification requirements for giving consent to the provision of information society services (ISS). Such a provision already exists under Article 8 of the UK GDPR, and the scope to give the government powers to introduce a requirement that already exists is elusive.

On the other hand, this new powers introduces new risks, and upsets existing and well-established legal safeguards. The Secretary of State would have the power to mandate specific age verification methods, which could potentially breach proportionality considerations dictated by UK data protection law and the European Convention of Human Rights. This power could also be used to pre-empt the outcome of the ongoing government consultation on digital identity, which could be designated as a mandatory mean to verify users' age.

Finally, the amendment confers unusually broad authority to amend, repeal, or modify any provision of UK data protection legislation—including foundational elements like data protection principles, data subject rights, and international transfer provisions—for age verification purposes. Introducing such expansive and unfettered powers is unnecessary for age verification purposes, and could inadvertently jeopardise UK adequacy and the free flow of data with the EU.

The cost of losing adequacy has been estimated to £1.6 billion for business compliance, which excludes the reduction in trade and exchange of services with the EU that would inevitably result.² Major EU-UK cooperation initiatives, such as the Trade and Cooperation Agreement, the Windsor Framework, and the UK participation to Horizon and Erasmus+, all depend on continued adequacy status.

Taken as a whole, this amendment appears to be a rushed-out exercise which lacks clear benefits, but introduces significant risks instead. Thus, Open Rights Group recommend to vote against a proposal that was drafted poorly and in haste.

Alternatively, we urge the House to support Amendment (e) – Proportionality Requirement for Regulations under sections 214A and Article 8ZA, as proposed by Liberty in their briefing. This amendment would, at least, address some of the most pressing concerns surrounding proportionality of age verification methods.

² See New Economic Foundation, *The cost of data inadequacy*, at: <https://neweconomics.org/2020/11/the-cost-of-data-inadequacy>