DATA USE AND ACCESS BILL

Briefing to the House of Lords Second reading

Author: Mariano delli Santi mariano@openrightsgroup.org

IN THIS BRIEFING

0. EXECUTIVE SUMMARY

The new Data (Use and Access) Bill drops several concerning aspects of the previous Data Protection and Digital Information Bill. Open Rights Group welcomes this as a positive development and a step in the right direction. In particular, we welcome the removal of provisions that would have: watered down the definition of personal data; expanded the scope of democratic engagement; lowered the threshold to refuse a data rights request to "vexatious and excessive"; removed various accountability requirements; allowed the Secretary of State to dictate the Strategic Priorities of the new Information Commission; required individuals to contact an organisation before lodging a formal regulatory complaint; removed the abolition of the Biometric and Surveillance Camera Commissioner.

Unfortunately, the Data (Use and Access) Bill still includes several provisions that would lower important protections for our data protection rights, and threaten public trust toward the use and deployment of new technologies such as Artificial Intelligence.

Maintaining robust data protection standards is a necessary condition to enable innovation and economic growth. Empowering individuals with strong data protection rights protects the public from extractive and exploitative business practices, thus ensuring that data uses lead to mutually beneficial outcomes and sustainable growth. High data protection standards are also an important enabler of digital identity services, smart data schemes, and the use of data to improve public services. The public need confidence that when they use a digital verification service, an online banking service, or when they visit a General Practitioner, the data they provide will be used for the reason they intended. The public also need confidence that the deployment of new technologies will not constrain their rights or their avenue for redress, and that strong regulatory supervision is in place to proactively mitigate and prevent risks. However:

1. **The Bill would remove important protections for automated decision-making and AI.** Article 22 of the UK GDPR enshrines the right not to be subject to a based on solely automated processing that have legal or otherwise significant effects on the individuals concerned. This right has proven to be a highly effective right that protects individuals from harmful decisions and discrimination. However, Clause 80 of the Data Bill would deprive individuals of this important right in most circumstances, and exacerbate power imbalances by requiring individuals to scrutinise, contest and assert their rights against decisions that were taken by systems outside of their control.
2. **The Bill would reduce transparency, particularly in the field of Artificial Intelligence.** Clauses 77 and 78 would reduce the scope of transparency obligations and rights. In particular, Clause 78 would effectively favour the

irresponsible development of AI products by allowing organisations which deploy those systems to comply with Subject Access Requests only if a "reasonable search" is needed to do so: thus, it allows it ignore SARs to the extent the AI system was designed in a way that makes it difficult to search data and comply with such requests. Further, if an organisation's capacity to handle requests becomes a consideration for the extent to which a SAR must be complied with, this would introduce a perverse incentive: an organisation with poor data management practices would find it difficult and resource intensive to comply with transparency obligations but, since their capacity to comply defines the extent of their obligation, they would get away with it.

3. **The Bill provides arbitrary and unaccountable powers to the Secretary of State.** The Data Bill introduces several clauses that would allow the Secretary of State to override primary legislation and modify key aspects of UK data protection law, including data sharing, via Statutory Instrument, without meaningful parliamentary scrutiny. These powers are being introduced in the absence of a meaningful justification and, in the words of the House of Lords, they "make it harder for Parliament to scrutinise the policy aims of the bill and can raise concerns about legal certainty".[1] Further, these powers were identified by the EU stakeholders as a main source of concern, and constitute a major threat to the continuation of the UK adequacy decision and the smooth functioning of the EU-UK Trade and Cooperation Agreement.
4. **The Bill lowers accountability over how data is shared and accessed for law enforcement and other public security purposes.** The Data Bill would remove the requirement to consider the legitimate expectations of the individuals whose data is being processed, or the impact on their rights, for a wide range of purposes such a national security, crime detection, safeguarding, or answering to a request made by a public authority. Further, the Data Bill would remove the requirement for law enforcement authorities to record the reason they are accessing data from a police database.
5. **The Bill is a missed opportunity to address the issues that plague the Information Commissioner's Office**, as they were highlighted in ORG's research released on 14 November.[2] While the new Data Bill have achieved some, limited but welcome, improvements on the prior Bill, it still carries over several problematic clauses from the DPDI Bill. This include the introduction of new primary and secondary objectives, the requirement to consult the Secretary of State before laying down a code of practice, and the appointment of the non-executive members of the new Information Commission.

---

1 Delegated Powers and Regulatory Reform Committee, *Democracy Denied? The urgent need to rebalance power between Parliament and the Executive*, at: https://publications.parliament.uk/pa/ld5802/ldselect/lddelreg/106/10602.htm

2 Ohrvik-Scott, J; Killock, J; delli Santi, M. Open Rights Group, *ICO Alternative Annual Report 2023-4" (2024)*, London. p. 9-15 https://www.openrightsgroup.org/publications/ico-alternative-annual-report-2023-24

Further, ORG is concerned by the lack of meaningful engagement with civil society and other critical stakeholders that has preceded the publication of this Bill by the new government. While it is clear that some of the previous criticism has been productively received and addressed, the government seem to underestimate the biases in the proposals from the previous administration. By rushing through legislative proposals developed and discussed under these circumstances, the government is taking steps that work against its stated intent of unlocking the use of data to promote growth, improve public services and make lives easier.

We urge the government and the House of Lords to allow meaningful scrutiny of this Bill to address the shortcomings it still inherited from the previous, ill-conceived Data Protection and Digital Information Bill. In particular, we recommend that:

- **The rights under Article 22 of the UK GDPR should be expanded to partly automated decision-making:** Drop Clause 80 (Automated decision-making), and consider extending the scope of Article 22 to partly automated decisions.
- **Obligation and transparency rights should not be compromised:** Drop Clauses 77 (Information to be provided for data subjects) and 78 (Searches in response to data subjects' requests).
- **Maximise legal certainty and ensure that any delegated legislative power is subject to appropriate safeguards and judicial scrutiny:** Drop, or change the nature of, Clauses 70 (lawfulness of processing), 71 (the purpose limitation), 74 (processing of special categories of personal data), 80 (automated decision-making), 85 (Safeguards for processing for research purposes etc) and Schedule 7 (Transfers of personal data to third countries etc: general processing), and ensure that the use of delegated legislative powers is left open to judicial challenge.
- **Accountability for access to data for law enforcement purposes should not be lowered, and data sharing should be underpinned a robust test to ensure individuals' rights and expectations are not disproportionately impacted:** Drop Schedule 4 (Lawfulness of Processing: recognised legitimate interests), Schedule 5 (Purpose limitation: processing to be treated as compatible with the original purpose) and Clause 81 (logging of law enforcement processing).
- **We urge to drop the ill-conceived changes proposed by the previous government, and seize this opportunity to address some of the core structural deficiencies that have emerged in the way the ICO operates and is held accountable:** Drop Clauses 90 (Duties of the Commissioner in carrying out functions), 91 (Codes of practice for the processing of personal data) and Schedule 14 (The Information Commission), and seize this opportunity to address some of the core structural deficiency that have emerged in the way the ICO operates. Alternatively, the government should consider a new consultation to address the ICO reform with a new legislative proposal.

1. THE BILL (STILL) REMOVES IMPORTANT PROTECTIONS FOR AUTOMATED DECISION-MAKING AND AI

Open Rights Group welcomes the government decision to remove clauses from the previous Data Protection and Digital Information Bill that would have lowered the threshold to refuse a rights request from "manifestly unfounded and excessive" to "vexatious and excessive". This new threshold would have applied to the right not to be subject to a solely automated decision, as well as to any other rights as established under UK data protection law—thus affecting the level of protection to personal data used by Artificial Intelligence systems as well as for any other use. Lowering the threshold that allows an organisation to refuse a rights request would only make it more difficult to ensure accountability against untimely, incomplete or unsatisfactory answer to a rights' request, thus heightening instead of reducing the imbalance of powers between individuals and organisations.

Article 22 of the UK GDPR enshrines the right not to be subject to a based on solely automated processing that have legal or otherwise significant effects on the individuals concerned. This is not an absolute prohibition: individuals can decide to be subject to solely automated-decision making either by giving their consent, or by validly entering into a contract that requires it. Parliament can also authorise by domestic law the use of a solely automated system in specific circumstances, and provided that such law enshrines "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests". Finally, Article 22 provides that and individual who is subject to a solely automated-decision must have "at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision".

Article 22 has proven to be a highly effective right that protects individuals from harmful decisions and discrimination. It has protected workers from unfair wage deductions and unfair dismissals.[3] It has protected individuals from being unfairly disadvantaged by their credit scoring.[4]

The importance to retain strong protections against automated decision-making is only bound to increase: a recent audit conducted by the ICO found that "AI is increasingly being used in the recruitment process to save time and money, helping to source potential candidates, summarise CVs and score applicants".[5] Likewise, public bodies such as the Department for Work and Pensions, whose algorithms

3 Workers Info Exchange, *Historic digital rights win for WIE and the ADCU over Uber and Ola at Amsterdam Court of Appeal*, at: https://www.workerinfoexchange.org/post/historic-digital-rights-win-for-wie-and-the-adcu-over-uber-and-ola-at-amsterdam-court-of-appeal

4 GDPRhub, *CJEU - C-634/21 - SCHUFA Holding (Scoring)*, at: https://gdprhub.eu/index.php?title=CJEU_-_C%E2%80%91634/21_-_SCHUFA_Holding_(Scoring)

have already falsely flagged 200.000 people for fraudulent activity,[6] are being given new powers to obtain bank account's data for fraud detection.[7] The Government has also expressed the intention to support the widespread adoption of AI tools by both public and private organisations.

However, the Data (Use and Access) Bill would deprive individuals of this important right in most circumstances, and exacerbate power imbalances by requiring individuals to scrutinise, contest and assert their rights against decisions that were taken by systems that are outside of their reach or control.

Clause 80 would remove Article 22 of the UK GDPR, and replace it with new Articles 22A, B, C and D. Under the new regime, individuals would lose their right not to be subject to automated decision-making, unless such decision is taken on account of sensitive data. Article 22D would also give discretion to the Secretary of State to designate automated decision-making systems which are exempt from the few safeguards that would still be enshrined in new Articles 22A, B, and C.

It is concerning that the government is proposing to remove or reduce safeguards around automated decision-making at a time when they are most needed. It is also concerning that the rationale expressed by the Government during a ministerial roundtable ORG attended is legally and logically faulty.

In particular:

- The government proposes to remove the prohibition to subject individuals to an automated decision without their consent as a means to favour the wider adoption of AI in society. However, this will only favour the unsafe deployment of AI and automated tools at the expenses of the welfare and well-being of the British public, who will instead be exposed to heightened risks of discriminatory and unfair decisions taken against them. In the long term, such a status quo will inevitably undermine public trust and societal acceptance of new technologies, thus creating a barrier to the deployment of AI rather than promoting it.
- The government has argued that Clause 80 provides clarity over when safeguards other than the right not to be subject to an automated decision would apply. This is incorrect, since new Article 22A, B and C do not provide any additional safeguard or clarity when compared to existing Article 22 of

5 Information Commissioner's Office, I*CO intervention into AI recruitment tools leads to better data protection for job seekers*, at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/11/ico-intervention-into-ai-recruitment-tools-leads-to-better-data-protection-for-job-seekers/

6 The Guardian, *DWP algorithm wrongly flags 200,000 people for possible fraud and error*, at: https://www.theguardian.com/society/article/2024/jun/23/dwp-algorithm-wrongly-flags-200000-people-possible-fraud-error

7 Gov.uk, *New laws to be introduced to crack down on fraud*, at: https://www.gov.uk/government/news/new-laws-to-be-introduced-to-crack-down-on-fraud

the UK GDPR. Thus, Clause 80 only removes safeguards that exist under today's rules, without providing any additional safeguards to compensate such removal.

- The government has argued that individuals would retain a right to opt-out of automated decision-making, thanks to the right to object provided by Article 21 of the UK GDPR. This argument is, however, incorrect: contrary to the right not to be subject to automated decision-making under article 22, which is unconditional, the right to object under article 21 can be overridden by the organisation on grounds related to their own interests. In turn, article 21 requires individuals to justify their opposition and prove that they have a right to object that prevails over the interests of the organisation, which may be difficult to do in practice and effectively shifts the onus on the individual rather than the organisation deploying the new system.

Recommendation: the rights under Article 22 of the UK GDPR should be expanded to partly automated decision-making.

Proposals to restrict the scope Article 22 rights are grounded on the false notion that lowering safeguards and safety standards would improve uptake and adoption of new technologies by the British public. Lowering regulatory standards would lower incentives to invest in the safe and trustworthy development of AI and automated systems, and will make it easier for organisations to transfer externalities onto the individuals instead.

We urge the House of Lords to:

- Drop Clause 80 from the Data (Use and Access) Bill.
- Introduce amendments that would expand the scope of Article 22 to partly automated decision-making, in line with the recommendation formulated by the Information Commissioner's Office in its repose to the Data a new direction consultation in 2021.[8]

8 Information Commissioner's Office, *Response to DCMS consultation "Data: a new direction"*, paragraph 34, at: https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf

2. THE BILL (STILL) REDUCES TRANSPARENCY, PARTICULARLY IN THE FIELD OF ARTIFICIAL INTELLIGENCE

Transparency is a fundamental right, as it enables control over personal data, and constitutes the first line of defence against unlawful uses of personal data. It allows individuals to understand how their data is being processed, the consequences of such processing, and to verify the legitimacy of data uses. Articles 12, 13, 14 and 15 of the UK GDPR give individuals the right to be informed and to access and receive a copy of their data. This is an unconditional right, which does not allow organisations not to answer or to answer only partially to such requests. Further, organisations cannot charge individuals for exercising their rights unless they can prove that their request is "manifestly unfounded or excessive".

However, Clauses 77 and 78 would reduce the scope of transparency obligations and right only to when providing information "would involve a disproportionate effort," and to information that can be retrieved "based on a reasonable and proportionate search". ORG is concerned that:

- **Clause 78 would effectively favour the irresponsible development of AI products by allowing organisations which deploy those systems to ignore Subject Access Requests, to the extent the system they use was designed in a way that makes it difficult to comply with such requests.** AI systems are notoriously designed in a way that makes it difficult to retrieve personal data once ingested, or understand how this data is being used. This is not due to technical limitations, but to a discrete decision of AI developers, who usually prioritise cost reduction over transparency and explainability.
- **If an organisation's capacity to handle requests becomes a consideration for the extent to which a Subject Access Request must be complied with, this would introduce a perverse incentive for organisations to collect excessive amount of personal data or adopt poor or suboptimal data management practices**, as doing so would effectively be rewarded rather than punished by the Data (Use and Access) Bill.

Recommendation: obligation and transparency rights should not be compromised.

As we move toward the adoption of Artificial Intelligence by the public and the private sector, retaining robust transparency obligations and right of access rights becomes an important first line of defence against potential misuses or bad outcomes.

We urge the House of Lords to:

- Drop Clauses 77 and 78 from the Data (Use and Access) Bill.

3. THE BILL (STILL) PROVIDES ARBITRARY AND UNACCOUNTABLE POWERS TO THE SECRETARY OF STATE

The Data (Use and Access) Bill introduces several clauses that would allow the Secretary of State to override primary legislation and modify key aspects of UK data protection law via Statutory Instrument. These include powers to:

- Introduce new legal bases for processing, known as "recognised legitimate interests" (Clause 70).
- Introduce exemptions to the purpose limitation principle, known as "list of compatible purposes" (Clause 71).
- Add or remove categories of data from the definition of what constitutes "special categories data", also known as sensitive data (Clause 74).
- Add or remove safeguards over the use of data for research purposes (clause 85) and over the use of data for solely automated decision making (Clause 80).
- Designate automated decision that are exempt from the safeguards provided by new Articles 22A, B, and C (Clause 80)
- Authorise transfers of personal data to third countries (Schedule 7).

The extent and arbitrariness of these powers is highly problematic:

- **These powers provide wide discretion to the Secretary of State without meaningful parliamentary scrutiny.** Indeed, "no SI has been rejected by the House of Commons since 1979".[9]
- **These powers are being introduced in the absence of a meaningful justification.** While the new Minister has opted not to express their views on this matter, the previous government argued that these powers were meant to allow Ministers to intervene if legislation was interpreted by the Courts in a way the government did not agree with. This is a faulty and dysfunctional rationale, that denies Parliament of its main prerogative—to write the laws that are meant to constrain what the government can do. Such a power can also be easily misused to interfere with, and bypass, a Judicial Review whose outcome the government does not like.
- **Henry VIII powers will, in the words of the House of Lords, "make it harder for Parliament to scrutinise the policy aims of the bill and can raise concerns about legal certainty".**[10] Further, Henry VIII powers should, in the words of the same report, "be recognised as constitutionally anomalous", and their use acceptable "only where there is an exceptional justification and no other realistic way of ensuring effective governance". None of these issues seem to

9 The Hansard Society, *Delegated legislation: the problems with the process*, p.16, at: https://www.hansardsociety.org.uk/publications/reports/delegated-legislation-the-problems-with-the-process

10 Delegated Powers and Regulatory Reform Committee, *Democracy Denied? The urgent need to rebalance power between Parliament and the Executive*, at: https://publications.parliament.uk/pa/ld5802/ldselect/lddelreg/106/10602.htm

have been addressed by the Data (Use and Access) Bill, where the breadth of the powers it confers does inherently reduce legal certainty and Parliament's ability to scrutinise legislation.

- **These powers were identified by the EU stakeholders as a main source of concern regarding the continuation of the UK adequacy decision, whose review is due in 2025.** The House of Lords inquiry into UK adequacy concluded that "lawful bases for data processing and the ability to designate legitimate interests by secondary legislation made by Ministers" constituted a significant concern for EU stakeholders and the continuation of the UK adequacy decision.[11] Henry VIII powers were also identified by the European Parliament review of the EU-UK Trade and Cooperation Agreement as a potential barrier to the functioning of such agreement.[12]
- **The risk these powers constitute to the UK adequacy decision are more than hypothetical:** for instance, if these powers were to be used, at any time, to authorise personal data transfers to a country that does not enjoy adequacy status from the EU, or to restrict the definition of special category data, this would guarantee the revocation or annulment of the UK adequacy status.

Recommendation: the new Data Bill should maximise legal certainty and ensure that any delegated legislative power is subject to appropriate safeguards and judicial scrutiny.

Delegated legislative powers reduce legal certainty, as they allow governments to change primary legislation according to the politics of the day. It also introduces significant risks for the retaining of the UK adequacy status: either these powers would never be used, and thus they don't need be provided, or they could be used in ways that put the UK adequacy status at risk.

We urge the House of Lords to:

- Reject Clauses 70, 71, 74, 80, 85 and Schedule 7, unless the government can justify reliance on delegated powers on grounds other than "a nice to have".
- If the need of establishing a delegated legislative power is justified, ensure that it is subject to clear restraints, and that the Secretary of State is not given unfettered discretion to override the rights and freedom of individuals. For instance, judicial scrutiny could be established by adopting a similar structure to Article 23 of the UK GDPR, that ensures exemptions to rights and freedom of the British Public can only be allowed if (and can be stricken down by a Court if they are not) limited, proportionate and subject to sufficient safeguards.

---

11 Lord Ricketts, *Letter to Rt Hon Peter Kyle MP re: UK-EU data adequacy*, at: https://committees.parliament.uk/publications/45388/documents/225096/default/

12 OPINION OF THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS (10.10.2023) within *REPORT on the implementation of the EU-UK Trade and Cooperation Agreement*, at: https://www.europarl.europa.eu/doceo/document/A-9-2023-0331_EN.html#_section11

4. THE BILL (STILL) LOWERS ACCOUNTABILITY OVER HOW DATA IS SHARED AND ACCESSED FOR LAW ENFORCEMENT AND OTHER PUBLIC SECURITY PURPOSES

A key aspect of data protection rests in how it restricts the use of personal data once it has been collected. The public needs confidence that their data will be used for the reasons they had shared them, and not further used in ways that breach their legitimate expectations—or they will become suspicious to providing their data.

However, Schedules 4 and 5 of the Data (Use and Access) Bill would remove the requirement to consider the legitimate expectations of the individuals whose data is being processed, or the impact this would have on their rights, for the purposes of national security, crime detection and prevention, safeguarding, or answering to a request made by a public authority. Data which is used for the purposes listed in these schedule would not need to undergo either a balancing test under Article 6(1)f, or a compatibility test under Article 6(4), of the UK GDPR.

Further, Clause 81 would remove the requirement for police forces to record the reason they are accessing data from a police database.

In turn, the combined effect of these provisions would be to authorise a quasi-unconditional data sharing for law enforcement and other public security purposes while, at the same time, reducing accountability and traceability over how the police uses the information they are being shared with. In turn, this risks further eroding trust in law enforcement authorities.

Likewise, a too-liberal approach to data sharing would also constitute a barrier to the adoption of digital verification services. For instance, fear that using a digital verification service may lead to personal data being shared with the Home Office for immigration control purposes, or with the Department of Work and Pension for a fraud check, would reduce trust and uptake in otherwise worthwhile schemes.

Recommendation: accountability for access to data for law enforcement purposes should not be lowered, and data sharing should be underpinned a robust test to ensure individuals' rights and expectations are not disproportionately impacted.

We urge the House of Lords to:

- Drop Schedules 4 and 5
- Drop Clause 81

5. THE BILL IS A MISSED OPPORTUNITY TO ADDRESS THE SHORTCOMINGS OF THE INFORMATION COMMISSIONER'S OFFICE

Proposals in the Data (Use and Access) Bill to establish an Information Commission as the UK data protector regulator have achieved some, limited but welcome, progress compared to the Data Protection and Digital Information Bill. In particular, Open Rights Group welcomes the removal of the power of the Secretary of State to issue a statement of Strategic Priorities that the new Information Commission should have had regard to when discharging its functions. ORG also welcomes the decision to retain the Office of the Biometric and Surveillance Camera Commissioner.

On the other hand, the new Data Bill still carries over several problematic changes that were proposed under the DPDI Bill, including:

- Introducing new, unclear and ultimately counterproductive primary and secondary statutory objectives of the new Information Commission (Clause 90).
- Introducing a new power for the Secretary of State to recommend the adoption or rejection of a Code of Conduct before the Information Commission is allowed to lay it before Parliament (Clause 91).
- Making every appointment of non-executive members of the Information Commission a Ministerial appointment, and thus consolidating the political and partisan nature of these appointments (Schedule 14).

None of these changes address, and in some cases they worsen, the status quo and the dysfunctionalities that the Information Commissioner's Office has been plagued with in the last decade. The Information Commissioner's Office (ICO) has a poor track record on enforcement. In 2021-22 it did not serve a single GDPR enforcement notice, secured no criminal convictions and issued only four GDPR fines totalling just £633k,[13] despite the fact that it received over 40,000 data subject complaints.[14] As Open Rights Group's "ICO Alternative Annual Report" shows, a lack of enforcement and weak regulatory oversight have persisted until today.[15]

13 See David Erdos, University of Cambridge, T*owards Effective Supervisory Oversight? Analysing UK Regulatory Enforcement of Data Protection and Electronic Privacy Rights and the Government's Statutory Reform Plans*, at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4284602

14 See Information Commissioner, *Annual Report and Financial Statements 2021-22*, pp. 42, at: https://ico.org.uk/media/about-the-ico/documents/4021039/ico-annual-report-2021-22.pdf

15 "ICO Alternative Annual Report 2023-4" (2024), Ohrvik-Scott, J; Killock, J; delli Santi, M. Open Rights Group: London. p. 9-15 https://www.openrightsgroup.org/publications/ico-alternative-annual-report-2023-24

Recommendation: the new Data Bill should move beyond the ill-conceived proposals of the previous government, and aim at addressing problems at the Information Commissioner's Office

Independent Data Protection Authorities are critical actors, tasked with the duty to safeguard civil liberties and individuals' rights by monitoring and enforcing compliance with data protection norms. DPAs are also meant to ensure that the rights of the British public find their enforcement and application where it may be difficult, time consuming or impractical to pursue justice autonomously.

We urge to drop the ill-conceived changes proposed by the previous government, and seize this opportunity to address some of the core structural deficiencies that have emerged in the way the ICO operates and is held accountable. ORG's recent research shows that the ICO is struggling to enforce data protection effectively, which distorts competition by rewarding bad actors, as well as failing people at risk from the abuse of their data.[16] In particular, the new Data Bill should:

- Clarify that the full and diligent enforcement of data protection laws constitutes the primary responsibility of the new Information Commission;
- Increase its arms-length body from the government, in particular by transferring budget responsibility and the appointment process of the non-executive members of the Information Commission to the relevant Select Committee, or else, giving the Committee a veto on appointments; [17]
- Provide for oversight of the ICO from the Equalities and Human Rights Commission;[18]
- Protect the Information Commission from cronyism and undue corporate influence, such as by introducing a two-years stay period to preclude members of the new Information Commission from working for the industries they regulated during their term for a period of two years;
- Allow effective judicial scrutiny of the new Information Commission regulatory function, in particular by extending the scope of orders under Section 166 of the Data Protection Act to the appropriateness of the Commissioner's response to a complaint; [19]and establish an "information rights ombudsman", to ease pressure on the Tribunal system; [20]
- Fully implement Article 80(2) of the UK GDPR and allow not-for-profit organisations to lodge representative complaints.

16 Ibid, p. 20
17 Ibid, pp. 25-26
18 Ibid, pp. 24-26
19 Ibid, p. 22-23, 26
20 Ibid, p.25-26

Published by Open Rights, a non-profit company limited by Guarantee, registered in England and Wales no. 05581537. The Society of Authors, 24 Bedford Row, London, WC1R 4EH. (CC BY-SA 4.0).

About Open Rights Group (ORG): Founded in 2005, Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect individuals' rights to privacy and free speech online. ORG has been following the UK government's proposed reforms to data protection since their inception.