OPEN RIGHTS GROUP ANALYSIS: THE UK DATA PROTECTION AND DIGITAL INFORMATION BILL

19 OCTOBER 2022

Contents

0. Executive summary

During the Conservative Party Conference 2022, the new UK Secretary of State for Digital announced plans to replace the GDPR with "a truly bespoke, British system of data protection".[1] This means that the UK Data Protection and Digital Information Bill (DPDIB), which this document summarises, will likely become superseded by a new proposal.

Yet, there is a common thread that binds the National Data Strategy (2020),[2] the TIGRR report[3] and the Data: a new direction consultation (2021)[4] or the DPDIB (2022): in each case, the Government have been quite outspoken in their intention to reform data protection to "simplify overcautious rules", "free up the use of data", reduce administrative burdens, and make the United Kingdom a "bridge across the Atlantic and operate as the world's data hub". Then, the DPDIB becomes the latest reiteration of this protracted effort and provides a useful overview of trends and issues that will likely re-emerge in the next proposal.

Having this in mind, we compare the DPDIB against the existing UK data protection framework, and in particular:

- **In section 1 (Main findings and recommendations)** we take stock of the findings in this report, and we recommend the Government not to present another Bill but to shelve their plans to reform data protection instead.
- **In Section 2 (Lawfulness and purpose limitation)** we explain how the Bill would empower the Secretary of State to introduce new

[1] Michelle Donelan, Our plan for digital infrastructure, culture, media and sport: https://www.conservatives.com/news/2022/our-plan-for-digital-infrastructure--culture--media-and-sport

[2] Policy Paper, National Data Strategy: https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy

[3] Taskforce on Innovation, Growth and Regulatory Reform: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/994125/FINAL_TIGRR_REPORT__1_.pdf

[4] Data: a new direction: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf

lawful grounds for processing and new exemptions that would legitimise data uses regardless of the circumstances or the impact this may have on individuals. We also explain why this new regulatory-making power would lack meaningful democratic scrutiny.

- **In Section 3 (Individuals' rights)** we explain how the Bill would weaken data protection rights, the right not to be subject to solely automated decisions, and the right to lodge a complaint. We also cover proposals to lower protections against widespread online surveillance via cookies or related technologies.
- **In Section 4 (Accountability framework)** we explain how the Bill would lower legal certainty over accountability requirements and the independence of Data Protection Officers (renamed Senior Responsible Individuals).
- **In Section 5 (Definition of personal data, UK representatives and International data transfers)** we explain how the Bill would weaken the definition of personal data and remove the requirement to appoint a UK Representative for oversea organisations. We also explain why the Bill would lower protections for personal data transferred abroad, and give discretion to the Secretary of State to approve international transfers regardless of the existence of enforceable rights and effective remedies.
- **In Section 6 (Independent supervision)** we explain how the Bill would impair the full and effective enforcement of data protection laws by the Information Commissioner's Office, and would give the Secretary of State the power to give instructions and interfere with the functioning of the ICO.

1. Main findings and recommendations

The the UK Data Protection and Digital Information Bill (DPDIB) would weaken legal standards, hinder the exercise of rights, water down accountability requirements, and introduce loopholes in the law. At the same time, Ministerial powers would be unduly expanded, enabling the Government to co-opt the Information Commissioner and bend primary legislation to their likes.

There is more to that. The UK currently benefits from an adequacy decision, which ensures the free flow of data toward the EU based on an assessment that found the UK GDPR to provide an "essentially equivalent level of protection" to the EU GDPR. However, of the 113 clauses of the DPDIB, we didn't find any that would raise UK data protection standards, but plenty that would substantially lower such protections. Thus, if the Government were to pursue these proposals, the adequacy decision would be in jeopardy and the UK digital sector with it: conservative estimates found the cost of data inadequacy to be likely to match 1 to 1.6 billion pounds in legal fees alone. This figure, which already outweighs the most optimistic expectations of the Bill,[5] does not compute the cost resulting from disruption of digital trade, investments, and relocation of UK businesses to the EU.[6]

While we leave the details to the full Report, it is useful to discuss about the circumstances that lead to what has already become an announced disaster.

The Data Protection and Digital Information Bill is the by-product of the Government decision to cherry-pick which organisations to engage with,

[5] Gov.UK, Data Protection and Digital Information Bill: Impact assessments: https://www.gov.uk/government/publications/data-protection-and-digital-information-bill-impact-assessments

[6] See Back to EU, While the UK has now left the EU, Cronofy is about to re-join. The UK government's plans to weaken data privacy laws is the final straw: https://adambird.com/posts/back-to-eu/

and their failure and unwillingness to listen to criticism. Indeed, more than 30 civil society organisations wrote to the former Secretary of State, denouncing the Data: a new direction consultation as rigged and potentially unlawful process.[7] Had the Government listened, they would have found that "There is consistent evidence of public support for more and better regulation", and that the public expects innovation to "be ethical, responsible and focused on public benefit".[8] In other words, the exact opposite of what the Government would deliver with this Bill.

The distance of the Government from the reality becomes more astounding when compared against the work of the Norwegian Privacy Commission. Like the UK, Norway is not an EU member state but has adopted the General Data Protection Regulation. And like the UK, they carried out a review of their domestic data protection framework, reaching the opposite conclusions of the UK Government.[9] In particular:

- Where the UK Government always characterised data protection legislation in terms of regulatory burdens, the Norwegian Privacy Commission (henceforth, the Privacy Commission) reasserted the need of recognising privacy "as a social good that has a fundamental value" and "a prerequisite for an open society and a well-functioning democracy".
- Where the UK Government proposed to reduce risk-aversion in the use of data, the Privacy Commission stressed the importance of risk-assessments and the need to apply "the precautionary principle [...] in cases where the use of technology entails a

[7] Techmonitor AI, Data Reform Bill consultation 'rigged' say civil rights groups: https://techmonitor.ai/policy/privacy-and-data-protection/data-reform-bill-consultation-dcms-nadine-dorries

[8] Who cares what the public think? UK public attitudes to regulating data and data-driven technologies: https://www.adalovelaceinstitute.org/evidence-review/public-attitudes-data- regulation/

[9] Norwegian Privacy Commission – Machine Translated Introduction: https://cryptpad.fr/pad/#/2/pad/view/7fsnWB617mUK9rqZoHS7xQ-9r5zludWz9Vp7feCHi14/
For the original, see: https://www.regjeringen.no/no/dokumenter/nou-2022-11/id2928543/?ch=3

particularly high risk to privacy".

- Where each of the proposals included in the Data Protection and Digital Information Bill are aimed at overriding retained EU law and lowering the protection of personal data afforded to UK residents, the Privacy Commission recommended "to use the national room for action that EU legislation provides, both to supplement the European rules, support [...] and to strengthen current EU legislation".

The UK Government failed to recognise the central role that data protection plays in modern, digitised societies, and the importance of robust regulation to clarify how innovation can take place within an ethical and sound framework. Unfortunately, this is a consistent trend the Government have shown with their Plan for Digital Regulation[10] up to their recent Approach to Regulating AI.[11]

All of the above leads to the same conclusion. The proposals of this Bill are unfit for purpose, dangerous, and damaging for the reputation of the UK. These data protection reforms are in no shape to be discussed in Parliament, nor the Government have shown the ability to understand this subject or legislate in this area. The Government should not pursue these reforms.

[10] Open Rights Group submission to the Department of Digital, Culture, Media and Sport — Plan for Digital Regulation: https://www.openrightsgroup.org/publications/open-rights-group-submission-to-the-department-of-digital-culture-media-and-sport-plan-for-digital-regulation/

[11] ORG response to the DCMS policy paper "Establishing a pro-innovation approach to regulating AI": https://www.openrightsgroup.org/publications/open-rights-group-response-to-the-dcms-policy-paper-establishing-a-pro-innovation-approach-to-regulating-ai/

2. Lawfulness and purpose limitation

In the UK GDPR, personal data must be processed under the conditions set by six lawful grounds for processing (Article 6). Lawful grounds are meant to define the boundaries of what data uses are legitimate, and to provide safeguards against abuses.

Furthermore, honouring individuals' reasonable expectations helps clarify the extent and consequences of data uses, thus promoting trust and legal certainty. In the UK GDPR, this is reflected by the principle of purpose limitation: personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

The UK GDPR also recognises some exceptions, in recognition of the social value of research activities or for public interest purposes:

- Article 5(1)b allows the further use "for archiving purposes in the public interest, scientific or historical research purposes", subject to appropriate safeguards;

- Article 23 allows the reuse of data for incompatible purposes for reasons of general interests, as well as the restrictions of other principles and rights. However, it mandates such exemptions to be narrowly construed.

In the following sections, we compare these principles against the changes introduced by the Data Protection and Digital Information Bill, and we explain why:

- **Clause 5** would introduce the new lawful ground of "recognised legitimate interests" that would eliminate the need to carry out a "balancing test". At the same time, it would empower the Secretary

of State to designate a "recognised legitimate interest", regardless of whether it trumps the rights and freedom of individuals, or the need to provide children with special protection.

- **Clause 6** would introduce a list of compatible purposes that would eliminate the need to carry out a "compatibility test" and empower the Secretary of State to exempt data uses from the purpose limitation principle, regardless of whether this is "a necessary and proportionate measure in a democratic society".

- **Clauses 9 and 22** would significantly widen the scope of the transparency exemption for research, archiving or statistical purposes, empower the Secretary of State to amend the safeguards that must apply to data processing for research purposes.

- Further, we explain why Clauses 5, 6 and 22 would empower the Secretary of State to amend primary legislation without meaningful accountability or democratic scrutiny.

2.1 Clause 5: Recognised legitimate interests vs Lawfulness

Clause 5 of the Data Protection and Digital Information Bill (DPDIB) would introduce a new lawful ground under new Article 6(1)ae, and the power for the Secretary of State to designate a list of “recognised legitimate interests” via Statutory Instrument.

Annex 1 of the DPDIB already provides a list of "recognised legitimate interests", which legitimises data uses for a number of reasons, including:

- “making a disclosure” to a public authority,

- “safeguarding” or “protecting public and national security,

- “detecting, investigating or preventing crime” and “apprehending or prosecuting offenders”.

These changes would:

- **Eliminate the need to carry out a balancing test.** Under the existing “legitimate interest” lawful ground,[12] Organisations must consider upfront the impact of data use on individuals and the measures to implement to mitigate such impact. Instead, data processing for a "recognised legitimate interest" would be legitimate regardless of the impact on the rights and freedom of the individuals affected, their reasonable expectations, or the existence of compelling reasons that justifies data processing.

- **Empower the Secretary of State to designate a “recognised legitimate interest”, regardless of whether it trumps the rights and freedom of individuals, or the need to provide children with special protection.** Under the existing "legitimate interest" lawful ground, data uses are not legitimate if there is an overriding right or freedom of the individuals affected. Instead, "recognised legitimate interests" can be designated "where the Secretary of State considers it appropriate to do so". The Secretary would only need to have regard, "among other things", to the "interests and fundamental rights and freedoms of data subjects" or "the need to provide children with special protection".

2.2 Clause 6: List of compatible purposes vs Purpose limitation

Clause 6 of the Data Protection and Digital Information Bill would introduce new Article 8A. This would empower the Secretary of State to designate a list of conditions in which processing is treated as compatible with the original purpose of processing via Statutory Instrument.

Annex 2 of the DPDIB already provides a list of "compatible purposes",

[12] Article 6(1)f of the UK GDPR

which legitimises data reuses for a number of reasons, including:

- “making a disclosure” to a public authority,
- “safeguarding” or “protecting public and national security,
- “detecting, investigating or preventing crime” and “apprehending or prosecuting offenders”,
- “the assessment or collection of a tax or duty or an imposition of a similar nature”.

These changes would:

- **Eliminate the need to carry out a "compatibility test"**, thus legitimising the reuse of personal data regardless of the original purpose, the context in which personal data was collected, or the existence of appropriate safeguards.
- **Empower the Secretary of State to exempt data reuses from the purpose limitation principle, regardless of whether this is "a necessary and proportionate measure in a democratic society".** Under Article 23 of the UK GDPR, legislative measures can introduce exemptions only "when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society". Also, exemptions must be narrowly construed and specify, where appropriate, the extent and scope to which such exemption would apply (what kind of data, what organisations could receive the data, the storage period etc...), and safeguards to prevent abuse or unlawful access or transfer. Instead, new Article 8A would empower the Secretary of State to designate data reuses that are to be treated as compatible with the original purpose whenever the Secretary "considers that processing in that case is necessary to safeguard an objective" of public interest.

2.3 Clause 9 and Clause 22: Research, Archive and Statistical purposes vs Suitable safeguards

Clause 9 of the Data Protection and Digital Information Bill (DPDIB) would amend Article 13 of the UK GDPR, and introduce an exemption to transparency obligations in favour of data processing for Research, Archive and Statistical purposes (RAS purposes). This exemption would require that "providing the information is impossible or would involve a disproportionate effort". This would:

- **Significantly widen the scope of the transparency exemption for RAS purposes.** Under existing Article 14 of the UK GDPR, such an exemption already exists but only where "personal data have not been obtained from the data subject". Instead, clause 9 would extend this exemption to personal data obtained directly from an individual.

- **Introduce a new definition of "disproportionate effort" that is not justified by the objective difficulty of contacting an individual.** Under existing Article 14 of the UK GDPR, a disproportionate effort occurs when providing information to the individuals would be "likely to render impossible or seriously impair the achievement of the objectives of that processing". Instead, clause 9 would define disproportionate effort as depending "on, among other things, the number of data subjects, the age of the personal data and any appropriate safeguards applied to the processing", regardless of the actual difficulty of contacting the individuals whose data was used.

Further, Clause 22 of the DPDIB would introduce new Articles 84A, 84B, 84C and 84D. These **would empower the Secretary of State to amend the safeguards that must apply to processing carried out for RAS purposes via Statutory Instrument.** In turn, the Secretary of State would be given the power to scrap or provide exemptions to the prohibition that forbids using personal data for RAS purposes "if the processing is likely to cause substantial damage or substantial distress", or "for the purposes of measures or decisions with respect to a particular data subject".

2.4 The powers of the Secretary of State lack democratic scrutiny

Finally, we saw how clauses 5, 6 and 22 would empower the Secretary of State to override primary legislation and introduce new lawful grounds for processing, or exemptions to the purpose limitation principle and to safeguards for research activities. This power can be used at the sole discretion of whether the Secretary of State "considers it appropriate", and would lack meaningful democratic or Parliamentary scrutiny. As a matter of fact:

- Only 17 statutory instruments (SIs) have been voted down in the last 65 years.
- The House of Commons has not rejected an SI since 1979.
- Not a single SI was defeated during the process of legislating for Brexit and Covid-19.

The same considerations apply to the regulatory-making powers of

- Excluding designated automated decision-making from the applicability of new Articles 22B and 22C (See further, Section 3.2).
- Introducing exceptions to cookies consent requirements (See further, Section 3.3).
- Authorising international data transfers by regulation (See further, Section 5.3).
- Issuing instructions to the ICO (See further, Section 6.2).

3. Individuals' rights

In the UK GDPR, individuals have rights that allow them to exercise greater control over the use of their personal data, thus mitigating power imbalances between individuals and organisations.

Further, providing actionable rights that individuals can use to control their data and to react to infringements of their rights helps translating data protection principles from theory to practice.

In the following sections, we compare these principles against the changes introduced by the Data Protection and Digital Information Bill, and we explain why:

- **Clause 7** would amend the threshold that enables organisations to refuse a request. This would exacerbate a sense of powerlessness amongst individuals, hindering their ability to exercise their rights while empowering organisations to intimidate them.

- **Clause 11** would expose individuals to solely automated decisions (ADM) against their will, watering down protections and shifting the burden of scrutinising ADMs on individuals.

- **Clause 79** would empower the Secretary of State to introduce exemptions from cookies consent requirements. This would facilitate some of the most harmful practices online, infringe the principle of data protection by design and by default, and fail to support technologies that automatically consent or object to online tracking and profiling.

- **Clauses 32 and 40** would give discretion to the ICO to refuse to act on complaints arbitrarily or make assumptions about the complainant's motives. Further, it would hinder the right to lodge a complaint, and expose complainants to intimidation and gaslighting from offenders.

3.1 Clause 7: Vexatious threshold vs Data protection rights

Clause 7 would lower the threshold for charging a reasonable fee or refusing a request from an individual to exercise their data protection rights from "manifestly unfounded or excessive" to "vexatious or excessive". This would:

- **Exacerbate a sense of powerlessness amongst individuals and hinder their ability to exercise their rights.** New Article 12A(4) provides a non-exhaustive list of circumstances to determine if a request is vexatious, including "the resources available to the controller" and "the extent to which the request repeats a previous request made by the data subject to the controller". However, a lack of resources or organisational preparedness to deal with a request does not indicate inappropriate use of data protection rights. Also, individuals may repeat their requests more than once to react to a similar violation of their right, or to compare the two responses. On the other hand, an organisation could use these grounds as a loophole to refuse a request to their advantage.
- **Legitimise organisations to intimidate individuals by inquiring or making assumptions about the reasons of their request.** New Article 12A(5) would allow organisations to refuse to act upon requests that "are intended to cause distress" or "are not made in good faith". However, the broad and speculative nature of some data rights (for instance, the right of access) does not make it appropriate to consider the intent behind these requests. Further, this would likely have a chilling effect on the exercise of data rights and disproportionately affect individuals in a position of vulnerability.
- **Be based on a false and meaningless comparison with the Freedom of Information regime.** The Government argued that the vexatious threshold "will bring [subject access requests] in line with the Freedom of Information regime" (FOIA). However, FOIA are broader in scope, as they enable individuals to seek access to "information held by public authorities or by persons providing services". Instead, data protection rights empower individuals to make requests only in relation to their personal data, making the scope of these requests inherently narrower.

3.2 Clause 11: New Article 22 vs The right not to be subject to solely-automated decision-making

Clause 11 would omit Article 22 of the UK GDPR and introduce new Articles 22A, 22B, 22C and 22D. these would

- Remove the right not to be subject to solely automated decisions that have legal or otherwise significant effects on them (with new Article 22C), unless the decision is based on special category data (with new Article 22B).

- Empower the Secretary of State (with new Article 22D) to exclude certain decisions from the scope of new Articles 22B to 22C, as well as to amend or omit the safeguards provided by Article 22C.

These changes would:

- **Expose individuals to solely automated decisions (ADM) against their will.** Existing Article 22 prohibits ADMs unless individuals gave their consent, they entered a contract, or unless it "is required or authorised by domestic law which also lays down suitable" safeguards. However, new Article 22B would restrict this prohibition to ADMs based on special category data, and new Article 22C would legitimise ADMs even if against the will of the individuals affected by this decision.

- **Be unfair, by watering down protections and shifting the burden of scrutinising ADMs on individuals.** Existing Article 22 requires meaningful human intervention because ADM systems can only be controlled and monitored by the organisation that deploys them. New Article 22C still provides the right to make representations, to obtain human intervention and to contest a decision. However, these rights would operate within a framework where ADMs are deployed without the consent of the individuals who are affected. It

is also unfair to require individuals to review and contest decisions taken by ADM systems they cannot possibly control or have access to.

- **Be irrational.** Solely ADMs can still have life-changing consequences even if they do not use special category data. Restrictions should be justified by the risk and impact these systems may have on individuals, not by the kind of data they use.

- **Empower the Secretary of State to arbitrarily exclude ADMs from the scope of Articles 22B and 22C regardless of their impact on the rights and welfare of the individuals concerned.** Further, and for our comment on the powers of the Secretary of State, see before, Section 2.4 The powers of the Secretary of State lack democratic scrutiny.

3.3 Clause 79: The powers of the Secretary of State vs The right to privacy in electronic communications

Clause 79(3) would give the Secretary of State the power to amend Regulation 6 of the Privacy and Electronic Communications Regulations (PECR), which prohibits storing information, or gaining access to information stored, in the terminal equipment of an individual without their informed consent such as by

- Providing exceptions to cookie consent requirements.

- Setting requirements on suppliers and providers of information technology to enable users of technology to automatically consent or object to cookies when visiting websites.

The Government argue that they would use these powers to move from an opt-in to an opt-out regime for cookies and other tracking technologies once solutions that allow individuals to automatically consent or object to cookies are widely available.[13]

[13] Consultation outcome, Data: a new direction – government response to

These changes would:

- **Facilitate and legitimatise some of the most harmful practices online.** Cookies enable widespread and uncontrolled surveillance and behavioural profiling of individuals, which have resulted in real-world harms such as predatory targeting of gambling addicts[14] or individuals with medical conditions.[15]

- **Infringe the principle of data protection by design and by default.** An opt-out model would make privacy-pervasive settings the new default, contrary to the requirements under Article 25 of the UK GDPR and in particular "that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons".

- **Fail to support technologies that automatically consent or object to online tracking and profiling.** The Government implied in their response that they would support browser-based or other automated solutions to express consent preferences "when available". However, automated consent tools are already available, but their adoption is discouraged by the lack of enforceability of these choices against websites and third parties. If the Government does not give legal enforceability for these signals, solutions will never be "widely available".

- **Empower the Secretary of State to arbitrarily exclude cookies from consent requirements, regardless of the level of risks they pose for the individuals concerned.** Further, and for our comment on the powers of the Secretary of State, see before, Section 2.4 The powers of the Secretary of State lack democratic scrutiny.

---

consultation:https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation

[14] New York Times, What a Gambling App Knows About You: https://www.nytimes.com/2021/03/24/technology/gambling-apps-tracking-sky-bet.html

[15] ICO, Catalogue retailer Easylife fined £1.48 million for breaking data protection and electronic marketing laws: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/10/catalogue-retailer-easylife-fined-148-million/

3.4 Clauses 32 and 40: Power of the Commissioner to refuse to act on certain complaints vs The right to lodge a complaint

Clause 32 would amend Section 135 of the UK Data Protection Act 2018, amending the threshold for the Commissioner to charge a reasonable fee or refuse a request from an individual or a data protection officer from "manifestly unfounded or excessive" to "vexatious or excessive"

Clause 40 would introduce a requirement for the complainant to attempt to resolve their complaint directly with the relevant data controller before lodging a complaint with the Information Commissioner's Office. Further, it would empower the ICO to refuse to act upon a complaint from an individual who did not try to resolve their complaint directly with the organisation before contacting the ICO. These changes would be complemented by Clause 39, which introduces a requirement for data controllers to have a simple and transparent complaints-handling process in place to deal with complaints.

These changes would:

- **Give discretion to the ICO to refuse to act on complaints arbitrarily, or by making assumptions about the motives of the complainant.** Existing Article 77 of the UK GDPR gives individuals the right to lodge a complaint, while Article 57 imposes a duty on the ICO to "handle complaints lodged by" an individual "and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period". By amending the threshold to refuse to act on a complaint from "manifestly unfounded" to "vexatious", individuals could see their complaints mishandled for reasons outside of their control, such as "the resources available to" the Commissioner, or the assumptions they make about the "good faith" of the complainant.

- **Hinder the right to lodge a complaint, and exacerbate a sense of powerlessness amongst individuals.** There are instances where the complexity and opaqueness of digital ecosystems make it difficult, if not impossible, to identify an organisation to complain against. By requiring individuals to reach out to the offender first, their right to lodge a complaint would be compromised when they need it most.

- **Expose complainants to intimidation and gaslighting.** The complaint-handling procedures of an offending organisation could be weaponised to misrepresent facts and discourage individuals from exercising their rights. This process also presents the risk of complainants making procedural mistakes that the ICO can weaponise to ditch their complaint.

4. Accountability framework

In the UK GDPR, the accountability framework promotes the enforcement and effective implementation of data protection rules by requiring organisations to record and produce documentation that demonstrates how organisations complied with data protection laws,

Further, accountability is also a proactive requirement, as organisations are required to carrying out assessments in order to identify harmful or discriminatory outcomes from the outset.

In the following sections, we compare these principles against the changes introduced by the Data Protection and Digital Information Bill, and we explain why:

- **Clause 14** would reduce the independence of the data protection officer (now senior responsible individual), reduce legal certainty over appointment criteria, and remove the duty of secrecy and confidentiality over the exercise of their function.

- **Clauses 17 and 18** would exclude the need to include a systemic description of the envisaged processing operation and the need to consult with those who are impacted by high risks data processing. Further, it would reduce legal certainty over the requirement to carry out risk assessments and legitimise data processing whose risks were not mitigated.

4.1 Clause 14: Senior Responsible Individual vs Independence of the data protection function

Clause 14 would remove the requirement to nominate a DPO and introduce new Articles 27A, 27B and 27C. These would require organisations to appoint a "senior responsible individual" to be responsible for the data

protection function, or to delegate that task to suitably skilled individuals. This new requirement would replace the requirements on data protection officers in Articles 37 to 39 of the UK GDPR and sections 69 to 71 of the 2018 Act. This would:

- **Reduce the independence of the data protection function.** Data Protection Officers must provide independent advice and in-house supervision. As such, they must operate without conflict of interest, while it is organisations (not DPOs) that are responsible for complying with the GDPR. However, the Senior Responsible Individual (SRI) would need to be part of "senior management": this would give them managerial interests as well as decision-making power on the purposes and means of the processing. Further, SRI would become responsible to "ensure compliance".

- **Remove the duty of secrecy and confidentiality.** DPOs must also provide advice on data protection rights to individuals and employees within an organisation. However, clause 14 would not replicate the privilege of being "bound by secrecy or confidentiality concerning the performance of" the data protection function. In turn, Senior Responsible Individuals could be weaponised by management.

- **Reduce legal certainty over the requirement to establish an independent data protection function.** The UK GDPR requires that a DPO is appointed in some circumstances, such as when an organisation carries out "regular and systematic monitoring of data subjects on a large scale" or processes "a large scale of special categories of data [...] or personal data relating to criminal convictions and offences". Instead, the Senior Responsible Individual would need be appointed only for "high-risk" data processing. This requirement lacks clarity and leaves too much discretion on the subjective assessment of the organisation that makes the appointment.

4.2 Clause 17 and 18: Risk-taking vs Data Protection Impact Assessments

Clause 17 would amend the heading of Article 35 of the UK GDPR from "Data Protection Impact Assessments" to "Assessments of high risk processing". Under the amended provisions, the data controller's assessment of high-risk processing would need to include:

- A summary of the purposes of the processing.
- An assessment of whether the processing was necessary and the risks it posed to individuals.
- A description of how the controller would mitigate any risks.

Furthermore, Clause 18 would remove the requirement under Article 36 of UK GDPR to consult the Commissioner before processing, where an assessment of high-risk processing indicated that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. Schedule 4 paragraph 10(2) would also amend Article 83 of the UK GDPR (general conditions for imposing an administrative fine) to allow the Commissioner to consider any relevant voluntary consultation under Article 36 when imposing administrative fines on a data controller.

These changes would:

- **Exclude the need to include a systemic description of the envisaged processing operation.** DPIAs under the UK GDPR should encourage organisations to think about data processing and its impact on individuals from the outset. However, by eliminating the need to produce a systemic description of the processing operation whose risk is being assessed, the effectiveness of the new "Assessments of high risk processing" in mitigating these risks is rather dubious. This also appears inconsistent with the principle of data protection by design and by default.

- **Exclude the need to consult with those who are affected by high risks data processing.** Organisations that carry out the DPIAs must "seek the views of data subjects or their representatives on the intended processing". However, the "Assessments of high risk processing" does not require these views to be sought or taken into account. This defeats the purpose of risk assessments, as the participation of the individuals being affected helps organisations to adopt a less subjective point of view. In turn, the resulting assessment of the risks should be more objective.

- **Reduce legal certainty over the requirement to carry out risk assessments.** A DPIA is always required when organisations conduct "a systematic and extensive evaluation of personal aspects [...] that produce legal effects", or "a systematic monitoring of a publicly accessible area on a large scale", or processes "a large scale of special categories of data [...] or of personal data relating to criminal convictions and offences". However, high risk assessments lack any prescriptive requirements, leaving the interpretation of high risk to the discretion and subjective point of view of the organisation carrying out the assessment.

- **Legitimise data uses whose risks were not mitigated.** Under the UK GDPR, prior consultation requires organisations that could not mitigate risks with a DPIA to seek advice from the ICO and abstain from commencing data processing until these risks have been mitigated (or the ICO authorised the processing). However, Clause 18 would make prior consultation a voluntary exercise, thus legitimising high risk processing even in the absence of mitigating measures.

5. Definition of personal data, UK representatives and International data transfers

Digital technologies and the Internet make it more likely that personal data may be stored or transferred to different organisations, or outside of the UK. Thus, ensuring that data protection rights "follow the data" is an essential safeguard against loopholes and data laundering. The UK GDPR achieves this objective by:

- Ensuring that personal data processing of individuals residing in the UK is subject to the provisions of the GDPR regardless of where the data is stored.

- Requiring overseas organisations to appoint a UK Representative acting as a point of contact and ensuring liability against UK law.

- Providing safeguards for international data transfers which ensure that personal data processed abroad are subject to an “equivalent level of protection”, and that individuals retain “enforceable rights and effective remedies”.

In the following section, we compare these principles against the changes introduced by the Data Protection and Digital Information Bill, and we explain why:

- **Clause 1** would substantially lower the protection afforded to personal data and be inconsistent with the ongoing nature of anonymisation.

- **Clause 13** would remove the requirement to appoint a UK representative. This would make enforcing UK data protection law harder, and hinder the exercise of data protection rights against overseas organisations.

- **Schedule 5** would give the Secretary of State discretion to authorise transfers for reasons other than the level of personal data protection. Further, it would eliminate the requirement to consider "public security, defence, national security and criminal law and the access of public authorities to personal data", the existence of an independent supervisory authority and effective judicial redress in assessing an "equivalent level of data protection". Finally, it may consider an international data transfer subject to appropriate safeguards even in the absence of enforceable rights and effective remedies.

5.1 Clause 1: Identifiability vs Protections that follow the data

Clause 1 would introduce new Section 3A in the UK Data Protection Act 2018, amending the definition of personal data. According to the new definition, information is personal data:

- “where the living individual is identifiable [...] by the controller or processor by reasonable means at the time of the processing ”,

- or “where the controller or processor knows, or ought reasonably to know, that another person will, or is likely to, obtain the information as a result of the processing, and the living individual will be, or is likely to be, identifiable [...] by that person by reasonable means at the time of the processing.”

These changes would:

- **Substantially lower the protection afforded to personal data.** Under the UK GDPR, data are considered anonymous based on an objective test of whether an individual "can be identified, directly or indirectly". However, with Clause 1, personal data could be considered anonymous merely on the basis of the circumstances

and resources available to an organisation, or their subjective assessment of whether another person would re-identify anonymised datasets.

- **Be inconsistent with the ongoing nature of anonymisation.** The effective anonymisation of data should be reassessed at reasonable intervals. However, Clause 1 only requires anonymity to be determined "at the time of processing".

5.2 Clause 13: UK representatives

Clause 13 would omit Article 27 of the UK GDPR. In turn, overseas organisations would no longer need to appoint a data protection representative within the UK.

This would:

- **Make it harder to enforce UK data protection law against overseas organisations**. The so-called extra-territorial scope of the UK GDPR means that UK data protection law applies to organisations that offer goods or services to individuals in the UK or otherwise handle their personal data, regardless of where they are established. Thus, Representatives under Article 27 ensure that organisations can be held liable for infringements of the UK GDPR. Indeed, the High Court of England and Wales concluded in its decision Sanso Rondon v LexisNexis Risk Solutions UK Ltd [2021] EWHC 1427 (QB), "The appointment by an Art. 3.2 controller of a representative is, in and of itself, an important signal that the controller is engaging with the GDPR, understands its scope provisions, and accepts the conditionalities it imposes on its access to data and data subjects".

- **Hinder the exercise data protection rights by individuals against oversea organisations.** UK representatives also act as the local point

of contact for an overseas organisation on "all issues relating to processing for the purpose of compliance with the [GDPR]". In turn, this ensures that individuals can liaise with representatives who understand the language and the law. Further, representatives will often provide advice about data protection to organisations that may otherwise not be aware of their duties and responsibilities under UK law.

5.3 Schedule 5: Transfers by regulation vs Essentially equivalent level of protection

Schedule 5 of the Bill would replace Chapter 5 of the UK GDPR, changing the UK's regime for international transfers. This would change the legal bases under which personal data could be lawfully transferred, in particular:

- New Article 45A would empower the Secretary of State to make regulations approving transfers of personal data to third countries or international organisations. This regime would replace adequacy regulations under the UK GDPR (for our comment on the powers of the Secretary of State, see before, Section 2.4 The powers of the Secretary of State lack democratic scrutiny).

- Under amended Article 46, organisations would be allowed to transfer personal data in countries without such regulation if they acted "reasonably and proportionately".

- New Article 47A would provide that "the Secretary of State may by regulations specify standard data protection clauses which the Secretary of State considers are capable of securing that the data protection test set out in Article 46 is met in relation to transfers of personal data generally or in relation to a type of transfer specified in the regulations".

These changes would:

- **Give discretion to the Secretary of State to authorise transfers for reasons other than the level of protection for personal data.** According to New Article 45B, in determining whether the data protection test is met "the Secretary of State may have regard to any matter which the Secretary of State considers relevant, including the desirability of facilitating transfers of personal data to and from the United Kingdom". This change must be seen in light of the intention to "boost trade" by "reducing barriers to data flows", including the possibility "to make adequacy regulations for groups of countries, regions and multilateral frameworks".[16] Further, and for our comment on the powers of the Secretary of State, see before, Section 2.4 The powers of the Secretary of State lack democratic scrutiny.

- **Eliminate the requirement to consider "public security, defence, national security and criminal law and the access of public authorities to personal data", the existence of an independent supervisory authority and of effective judicial redress.** All these requirements played a pivotal role in determining the invalidity of adequacy determination in the Schrems I and Schrems II judgements. Instead, new Article 45B only requires "respect for the rule of law and for human rights in the country or by the organisation", "the existence, and powers, of an authority responsible for enforcing the protection" and "arrangements for judicial or non-judicial redress" are considered in the data protection test.

[16] Consultation outcome, Data: a new direction – government response to consultation: https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation

- **Consider an international data transfer subject to appropriate safeguards even in the absence of enforceable rights and effective remedies.** According to Article 46 of the UK GDPR, appropriate safeguards must provide "enforceable data subject rights and effective legal remedies for data subjects". The enforceable nature of contractual clauses was identified as an essential element to ensure "appropriate safeguards" in the Schrems II judgement. However, Schedule 5 would amend Article 46 so that a transfer is considered to be subject to appropriate safeguards if an organisation acted "reasonably and proportionately", or if the Secretary of State specified standard data protection clauses under new Article 47A which "the Secretary of State considers are capable of securing that the data protection test". However, these criteria do not consider the actual existence of enforceable rights and legal remedies but only the due diligence of the organisation operating the transfer or the opinion of the Secretary.

6. Independent supervision

Independent Supervisory Authorities are critical actors, tasked with the duty to safeguard civil liberties and individuals' rights by monitoring and enforcing compliance with data protection norms.

Personal data processing can result in discrimination and harm that interfere with individuals' fundamental rights. Further, data protection often interferes with or supports other fundamental rights, such as the right to free speech, assembly or religion. This makes it extremely important that the monitoring and enforcement of data protection laws are objective and free from partisan or extra-legal considerations.

In the following sections, we compare these principles against the changes introduced by the Data Protection and Digital Information Bill, and we explain why:

- **Clause 27** would set new objectives to the role of the Commissioner, compromising their ability to enforce the GDPR "fully and with all due diligence.

- **Clauses 28 and 31** would empower the Secretary of State to issue instructions to the ICO, and to interfere with the objective and impartial functioning of the Commissioner.

6.1 Clause 27: Commissioner's role vs Effective enforcement

Clause 27 would insert new sections 120A and 120 into Part 5 of the 2018 Act, making changes to the Information Commissioner's role. In particular:

- New Section 120A would introduce the principal objective of

securing “an appropriate level of protection for personal data, having regard to the interests of data subjects, controllers and others and matters of general public interest, and to promote public trust and confidence in the processing of personal data.”

- New Section 120B would introduce additional duties for the Commissioner, such as to have regard for the desirability of "promoting innovation"; "promoting competition", or of "the importance of the prevention, investigation, detection and prosecution of criminal offences" and "the need to safeguard public security and national security".

These changes would compromise the ability of the Commissioner to enforce the GDPR “fully and with all due diligence”. Under the GDPR, Data Protection Authorities must "execute [their] responsibility for ensuring that the GDPR is fully enforced with all due diligence" and "monitor and enforce the application of this Regulation", such as by adopting measures that "should be appropriate, necessary and proportionate in view of ensuring compliance". However, the new role of the Information Commissioner would require balancing the enforcement of data protection laws against external interests, thus lowering the level of personal data protection it ensures.

6.2 Clauses 28 and 31: Powers of the Secretary of State vs Independent oversight

Clause 28 would insert new sections into Part 5 of the 2018 Act, empowering the Secretary of State to introduce a Statement of Strategic Priorities to which the Commissioner must have regard. In particular

- New Section 120E would empower the Secretary of State to “designate a statement as the statement of strategic priorities” that “sets out the strategic priorities of Her Majesty’s government relating to data protection”.

- New Section 120F would require the Commissioner to "have regard to the statement of strategic priorities" when discharging their function, as well as to publish a response explaining how they would regard the statement.

- New Section 120H requires the SoS to submit their draft statement of strategic priorities to Parliament for approval via the negative resolution procedure on a non-amendable motion.

Further, clause 31 would subject Codes of Practice to the prior approval of the Secretary of State before they can be laid before Parliament. In detail:

- New Section 124D(1) would require the Commissioner to submit the final draft of a code of practice to the Secretary of State;

- New Sections 124D(2) and (4) would give the power to the Secretary of State to reject the draft submitted by the Commissioner, and issue a statement that explains the reasons for such refusal;

- New Section 124D(5) would require the Commissioner to review their rejected code of practice in light of the statement issued by the Secretary of State.

At present, the Commissioner must issue Codes of Practice concerning "Data-sharing", "Direct marketing", "Age-appropriate design", and "Data protection and journalism". More codes can be requested by the Secretary of State under new Section 124A.

These changes would empower the Secretary of State to issue instructions to the ICO, and to interfere with their objective and impartial application of the law. The independence of supervisory authorities is considered one of the essential safeguards to ensure full objectivity by both EU and Council of Europe legal instruments. Data protection is a fundamental right that can interfere with or support other fundamental rights: thus, it is

imperative that monitoring and enforcement of data protection laws are objective and free from partisan or extra-legal considerations. However,

- The power of the SoS to issue a statement of Strategic Priorities the Commissioner must have regard to is clearly at stake with the principle that a Supervisory Authority must not take instructions from anybody.

- The power of the Secretary to approve, reject or issue a statement that explains what the Commissioner should change in a code of practice to receive approval is incompatible with the principle that a Supervisory Authority must act objectively, impartially, and remain free from any direct or indirect external influence.

Further, and for our comment on the powers of the Secretary of State, see before, Section 2.4 The powers of the Secretary of State lack democratic scrutiny.

7. About the Open Rights Group

Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 20,000 active supporters, we are a grassroots organisation with local groups across the UK. We were heavily involved in the process leading up to the enactment of the Data Protection Act 2018 ("DPA 2018"), and we worked on issues such as data retention, the use of personal data in the COVID-19 pandemic, data protection enforcement, online advertising and the use of personal data by political parties. We have litigated a number of successful data protection and privacy cases, ranging from challenges to the lawfulness of the Regulation of Investigatory Powers Act at the European Court of Human Rights,[17] being a party at the Watson case against UK data retention, through to the recent challenge against the Immigration Exemption in the Data Protection Act.[18] We are also supporting complaints made to the Information Commissioner regarding Adtech and the use of data by political parties.

[17] Open Rights Group, Court Rules UK Mass Surveillance Programme Unlawful: https://www.openrightsgroup.org/campaign/court-rules-uk-mass-surveillance-programme-unlawful/

[18] Open Rights Group, Immigration Exemption judged unlawful, excessive, wrong by Court of Appeal: https://www.openrightsgroup.org/press-releases/immigration-exemption-judged-unlawful-excessive-wrong-by-court-of-appeal/