OPEN RIGHTS GROUP RESPONSE TO DATA: A NEW DIRECTION

19 November 2021

EXECUTIVE SUMMARY

On 10 September 2021, the Department for Digital, Culture, Media and Sport (DCMS) published "Data: a new direction", a consultation about reforms to the UK data protection framework.

Open Rights Group (ORG) is deeply concerned by the contents and the potential impact of the proposals being discussed in this consultation. New technological developments have shown the potential to threaten our rights and discriminate at scale[1] and existing data protection laws provide for much needed legal protection and remedies against these risks, such as

- Obligations to use data responsibly, fairly, transparently, as well as to assess and mitigate the adverse or discriminatory consequences that such uses may have on individuals;
- Rights to know how personal data is being used, object to such uses, and ultimately retain control over life-changing data-driven decisions;
- Remedies for victims of abuses and independent oversight.

The importance of these rights for ensuring technological development can thrive, while at the same time safeguarding public trust and confidence in how organisations use our data, is undisputed. These are the same rules that supported the UK in becoming a "science superpower"; the home of a thriving digital sector. Yet, DCMS proposals persistently portray data protection as a burden and an obstacle that stands in the way of innovation. We stress the overall lack of convincing analysis or supporting evidence that underpin Government conclusions.

The result is a set of proposals that would

- Significantly undermine legal standards, and create loopholes that will be detrimental to "the trustworthy use of data";
- Disempower individuals, and
- Remove effective remedies and oversight against abuses.

Ultimately, these proposals directly contradict the Government's objective of "unleashing the power of data". Such power cannot be reconciled with a policy for

[1] Open Rights Group, *Open Rights Group submission to the Department of Digital, Culture, Media and Sport — Plan for Digital Regulation*. Available at: https://www.openrightsgroup.org/publications/open-rights-group-submission-to-the-department-of-digital-culture-media-and-sport-plan-for-digital-regulation/
See also: Solove, Daniel J. and Keats Citron, Danielle, "Privacy Harms" (2021). GW Law Faculty Publications & Other Works. 1534. https://scholarship.law.gwu.edu/faculty_publications/1534

“innovation” and “growth”. There is no substitute to a human dignity and fundamental rights lens to ascertain whether the “power of data” is being used to our benefit or against it. As the consultation shifts away from fundamental rights to an apparently wholly business-orientated approach, it ultimatey does business a disservice.

The relation between citizen and state or business must work on the basis of transparency and trust. The proposals would reduce trust, increase tangible abuse of data and result in negative outcomes for individuals. This would undermine the Government’s objectives to enhance and enable innovation. We explain, for instance, how the research proposals would lead to public distrust of scientific research activities, a core area identified for growth. Allowing wider, unpredictable uses of data, including nearly any business purposes that “improves customer service” without balancing the impacts on individuals, would further undermine public trust.

Yet the Government also seeks to liberalise the use of data sharing, not least through its competition policy. Following the lead of Open Banking, the Government wishes to encourage sharing of personal data for services, such as telephony or energy, through interoperable standards. However, it is essential to look at the bigger picture here. Without a firm, enforceable and predictable data protection framework, such efforts to push interoperability would look entirely untrustworthy. Thus the innovation the CMA (Competition & Markets Authority) or others would seek to promote, would be fatally undermined.

These proposals would also undermine initiatives like the Online Safety Bill. Personal data is used to prioritise content and to profile for advertising. Much of this is arguably unlawful. By making profiling of customers easy to justify, the proposals would fuel the very market failures that are leading to the problems the Online Safety Bill seeks to address.

The supporting approaches include making services more porous or ‘interoperable’ so that customers can better dictate their online environment and thereby reduce harms and other problems through the market. Such measures would also be fatally undermined by these proposals, as they rely on the ability of personal data to move across services.

The current data protection framework genuinely serves the Government’s objective of promoting innovation and competitive markets, by supporting and developing trust, predictability and transparency. The consultation document’s suggestions would undermine these objectives in a systematic manner.

ABOUT ORG

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 sucessful data protection and privacy cases, ranging from challenges to the lawfulneess of the Regulation of Investigatory Powers Act at the European Court of Human Rights,[2] 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.[3] We are also supporting complaints made to the Information Commissioner regarding Adtech and the use of data by political parties.

ABOUT THIS DOCUMENT AND ITS STRUCTURE

This document contains ORG's response to the consultation. ORG has responded to the questions within the consultation which it has particular interest in and /or expertise on.[4] ORG has followed the order of the questions as they appear in the consultation paper. A full list of the questions ORG has responded on is provided in the Table of Contents to follow. A non-response to a question does not represent any endorsement by ORG of the proposals that question relates to.

ORG has used the DCMS Chapter and section headings within its response for ease of use and cross-reference purposes. However, ORG has also included **alternative titles** for many of these headings, as a means to supplement and challenge the DCMS' framing of the issues.

At the beginning of each section, ORG presents a short introduction containing (i) a brief overview of the government's proposals (ii) ORG's key concerns and (iii) a summary of ORG's submissions on the issue. Following this, ORG provides its detailed responses to the consultation questions.

---

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

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

[4] These questions are contained in Chapters 1, 2 and 5 of the consultation.

TABLE OF CONTENTS

CHAPTER 1:
REDUCING BARRIERS TO RESPONSIBLE INNOVATION
(*OR* UNDERMINING THE RIGHT TO DATA PROTECTION)

1.2 RESEARCH PURPOSES (*OR* OVERSTRETCHING RESEARCH-SPECIFIC PROVISIONS)

Introduction

- The Government propose to consolidate and amend research provisions, expand the legal definition of "scientific research", and introduce a new lawful ground to use data for research purposes.

- ORG has concerns that the proposals risk overstretching research-specific provisions by enabling commercial and for-profit uses of personal data under the guise of "scientific research". In turn, this would strip individuals of important safeguards and risks undermining trust in legitimate research activities.

- These proposals are not necessary to help researchers and others to navigate regulatory requirements or ensure legal certainty. These issues could be adequately and appropriately addressed by guidance from the Information Commissioner.

Response

Q1.2.1 To what extent do you agree that consolidating and bringing together research-specific provisions will allow researchers to navigate the relevant law more easily?

Strongly disagree

Modifying the legal rules underpinning the use of data for research purposes is not necessary. Changes to the legal text of the UK GDPR are unlikely to bring further clarity to researchers who experience difficulties navigating and interpreting the law. Instead, researchers would benefit from clear and user-friendly ICO guidance on the research provisions and when they apply.

ORG does not agree with the government opinion, at §37, that guidance alone would not be sufficient. Plain English guidance will be more valuable to researchers than consolidating legal provisions in one place. Guidance can take into account the

specific needs of researchers who may lack a legal background, providing a step by step guide that they can follow.

Furthermore, ORG is aware of developments at a European level by the EDMO (European Digital Media Observatory) Working Group towards creating a code of conduct under Article 40 GDPR, with a view to facilitating access to platform data by researchers.[5] That Code is being developed in conjunction with British academics and lawyers. Such a Code represents a better pathway to supporting research than embarking on rigid legislative change.

Conversely, modifying the research-specific provisions risks undermining the protections afforded by existing legal rules. There is no evidence that the UK GDPR is creating barriers to innovation, and indeed the Government notes at §34 that "the UK is ranked second in the world for science and research".

Q1.2.2. To what extent do you agree that creating a statutory definition of 'scientific research' would result in greater certainty for researchers?

Strongly disagree

The UK GDPR already enshrines a clear definition of scientific research at Recital 159. There is no firm evidence that the definition provided by Recital 159 is unclear. Recital 159 has interpretative status and helps address uncertainties regarding what constitutes research by clarifying what kind of research activities fall under the UK GDPR regime for research purposes.

ICO guidance could further enhance legal certainty regarding the interpretation of scientific research without the need to change its legal definition. Moreover, ORG is aware of active developments towards creating an Article 40 GDPR Code of Conduct in this area, which could further help clarify definitional issues.

Creating a statutory definition of "scientific research" risks going beyond what people would reasonably expect to be covered by that term, for example creating a definition which encompassed commercial activities or for-profit interests. This could undermine public trust over the use of personal data for research purposes.

[5] EDMO, L*aunch of the EDMO Working Group on Access to Platform Data.* Available at: https://edmo.eu/2021/08/30/launch-of-the-edmo-working-group-on-access-to-platform-data/?utm_source=rss&utm_medium=rss&utm_campaign=launch-of-the-edmo-working-group-on-access-to-platform-data

Furthermore, a statutory definitions risks being rigid and constraining the research provisions to a certain type of research only. The definition of "scientific research" provided by Recital 159 is future-proofed because it is not exhaustive and can take into account societal and technological developments. This flexibility may be lost in a statutory definition. There is also a risk to having different legal standards between the UK and EU as this could jeopardise cross-border research projects.

Q1.2.6. To what extent do you agree that creating a new, separate lawful ground for research (subject to suitable safeguards) would support researchers to select the best lawful ground for processing personal data?

Strongly disagree

There is no need to introduce a new lawful ground for research purposes. Researchers can already rely on bases such as consent, legitimate interest, and public interest. There is no evidence that the existing legal bases cannot adequately accommodate researchers.

However to the extent that further clarity is needed, regulatory guidance from the ICO would be better suited to support researchers to select the best lawful ground for their research. This guidance could help researchers to consider which bases are appropriate for them and clarify how those legal bases apply in a research context. Guidance would support researchers in navigating legal requirements without impacting the important protections for individuals that are attached to those legal bases. Such guidance can be tailored to researchers' needs and made user-friendly - for instance, a step-by-step guide. Furthermore, ORG is aware that there are active developments towards creating a Code of Conduct in this area, which will clarify how legal bases apply to research.

Conversely, introducing a new lawful ground for research purposes would affect the protection afforded by the UK GDPR to individuals whose data are used for research purposes. This may permit irresponsible uses of data by organisations who would otherwise struggle to find a lawful basis for their activities. At the same time, it would reduce individuals' ability to control how their data is used for research purposes.

For instance, a “research” lawful basis would provide:

- An alternative to the lawful basis of “consent” (Article 6(1)a of the UK GDPR). In such case, this may undermine the individuals’ ability not to consent to a research activity they do not wish to participate in. For research activities where consent would otherwise be the legal basis, individuals would lose their ability to withdraw from research projects at a later stage.
- An alternative to the lawful basis of a “task carried out in the public interest” (Article 6(1)e of the UK GDPR). This could permit research that is not in the public good, and which would otherwise need to be justified under legitimate interests or through obtaining consent, to be easily conducted.
- An alternative to the lawful basis of “legitimate interests” (Article 6(1)f of the UK GDPR). In cases where legitimate interests would otherwise be the legal basis, it would remove the requirement of conducting a balancing test between the legitimate interests of the researcher (or other actor) and the rights and freedom of the individuals. Organisations would be allowed to trump the rights of individuals by claiming that they are conducting “scientific research”.

Enabling research to be conducted without consent, or without any assessment of whether it is in the public good, or any balancing of an organisation’s interests against the harms to individuals, is not a desirable outcome from the consultation. Rather than providing benefit to researchers, introducing a new legal ground that bypasses existing requirements would reduce trust and public support for scientific research.

1.3 FURTHER PROCESSING (*OR* ENABLING CREEPY USES OF DATA)

Introduction

- The Government propose to reform the limits on further processing which prohibit organisations from reusing personal data for reasons that are incompatible with their original purposes. This includes a proposal to permit incompatible further processing which is based on a law that safeguards an important public interest, and proposals to clarify when a new organisation who did not originally collect the data can further process data.

- These proposals would undermine the principle of purpose limitation, and risks exposing individuals to their personal data being used in ways which they cannot foresee. It is not clear how laws permitting incompatible uses of personal data for public interest reasons would be defined and what safeguards would apply to such laws. ORG has concerns this would give unprecedented power to the Government and / or private actors to interfere with the private life of UK residents, and that vulnerable groups, such as migrants, would be particularly affected.

- ORG submits that there is no need to amend the existing framework which already provides clarity and certainty on when data may be processed for incompatible purposes and which provides important protections to individuals against data misuse, such as function creep and mission creep.

Response

Q1.3.1 To what extent do you agree that the provisions in Article 6(4) of the UK GDPR on further processing can cause confusion when determining what is lawful, including on the application of the elements in the compatibility test?

Strongly disagree

Article 6(4) UK GDPR, when coupled with the guidance in Recital 50 concerning "the reasonable expectations of data subjects based on their relationship with the

controller as to their further use", provides clear and foreseeable guidance which assists controllers to appreciate when re-use may be compatible with the initial purpose of collection of data.

These are well worn concepts and there is no evidence to support the need for them to be changed. For example the compatibility test for further processing was included in the EU Data Protection Directive in 1995, and has been clarified in a Working Party Article 29 guidance on purpose limitation that was issued in 2013.[6] The first review of the implementation of the GDPR found no evidence that the compatibility test, now under article 6(4) of the UK GDPR, is an obstacle to the responsible use of data.[7]

Q1.3.2. To what extent do you agree that the Government should seek to clarify in the legislative text itself that further processing may be lawful when it is a) compatible or b) incompatible but based on a law that safeguards an important public interest?

Strongly disagree

It is not clear what an "important public interest" is as there is no definition proposed for this term. Nor is it clear how such a law would be defined. For instance, it is not made clear whether the tests of necessity and proportionality will be included, to ensure that the secondary processing is necessary to achieve the public interest and that the interference with privacy is proportionate to achieving that purpose. Unless such a law is tightly defined, it could circumvent essential protections to the rights of individuals, exposing them to harms and abuses of their rights. ORG has included **examples**, further below, of the types of impact which these changes might have on individuals.

The existing legal framework already contains exemptions from the purpose limitation principle. Thus, it is not clear why duplicative legal provisions are needed. Under Article 6(4), any processing which is based on a "domestic law which constitutes a necessary and proportionate measure in a democratic society to safeguard national security, defence or any of the objectives referred to in Article 23(1)" will be compatible.[8] Schedule 2 of the DPA 2018 provides for exemptions which

6 Working Party Article 29, *Opinion 03/2013 on purpose limitation*, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

7 COM(2020) 264 final, *Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*. Available at: https://ec.europa.eu/info/sites/default/files/1_en_act_part1_v6_1.pdf

8 Those objectives include:

are based on 23(1) and 6(3), including from the purpose limitation principle, for matters that are considered to safeguard a public interest, such as the "crime and taxation" exemptions and functions which are designed to protect the public.

Current exemptions from the GDPR's purpose limitation principle enshrine important protections for individuals. For example, Article 23 UK GDPR only permits deviations where the restriction *"respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard* [one of the interests set out in 23(1))]". Such a restriction must contain additional safeguards, such as:

- The requirement to exhaustively define the scope of the law and the kind of data that would be used under these conditions (Article 23(2)a, b, c).
- Safeguards to prevent abuse or unlawful uses, as well as limits over how long data can be stored (Article 23(2)d, g).
- Limits over what organisations can access or use the data in this manner (Article 23(2)e).

Furthermore, Article 6(3) UK GDPR only permits adaptions to the purpose limitation principle where the legal basis is grounded in a law that meets an objective of public interest and is proportionate to a legitimate aim or goal which is being pursued. These are important protections. However, amending the rules governing the further use of data for incompatible purposes may result in the bypassing of these protections and the introduction of laws that are not "necessary and proportionate measure in a democratic society" and which lack suitable safeguards for the rights and freedom of individuals.

(c) public security;
(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
(e) other important objectives of general public interest, in particular an important economic or financial interest of the United Kingdom, including monetary, budgetary and taxation a matters, public health and social security;
(f) the protection of judicial independence and judicial proceedings;
(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
(i) the protection of the data subject or the rights and freedoms of others;
(j) the enforcement of civil law claims.

Q1.3.3. To what extent do you agree that the Government should seek to clarify when further processing can be undertaken by a controller different from the original controller?

Strongly disagree

This would undermine foreseeability and the reasonable expectations of individuals. Organisations should not be seeking to process data in unexpected or unforeseeable ways. This is prevented due to the safeguards in the current regime.

Any reforms that seek to address processing by another entity that does not have a relationship with the individual will erode foreseeability. It will also create risks for controllers trying to comply with transparency obligations. This will be compounded by potentially enabling further onward transfers over which individuals would have diminishing levels of control. Instead, the original controller should seek a lawful basis for the further processing, if that processing is incompatible with the original processing purposes.

Q1.3.4. To what extent do you agree that the Government should seek to clarify when further processing may occur, when the original lawful ground was consent?

Strongly disagree

This would hollow the meaning of consent. Consent must be specific and informed to meet the UK GDPR standard. The original controller should be able to seek consent for the further processing, to the extent it is incompatible with the original purposes. Introducing a further layer of processing which is incompatible with the informed and specific consent provided by the individual would impoverish individual control while providing little benefit to responsible controllers.

1.4 LEGITIMATE INTERESTS (*OR* EXPOSING INDIVIDUALS TO HARM AND DISCRIMINATION)

Introduction

- The Government propose to create a limited, exhaustive list of legitimate interests for which organisations can use personal data without applying the balancing test. This would mean the certain activities are legitimised without needing to consider the impact on individuals.

- ORG has concerns that removing the balancing exercise would normalise uses of personal data which could result in harm and discrimination to individuals.

- ORG considers that ICO guidance could assist if there is uncertainty regarding the legitimate interests lawful ground. Issues with consent fatigue can be appropriately solved by enforcement of consent which does not meet the GDPR thresholds for consent. There is no need to amend the balancing exercise within the legitimate interests lawful basis to solve that issue.

Response

Q1.4.1. To what extent do you agree with the proposal to create a limited, exhaustive list of legitimate interests for which organisations can use personal data without applying the balancing test?

Strongly disagree

The proposals would shift the responsibility for conducting the balancing exercise from organisations to government. As the ICO observes, government and parliament *"would need to be confident in drawing up such a list that the types of processing included in it do not have a disproportionate impact on people's rights."* The ICO goes on to say that *"to have the required confidence, the nature, context and detail of the processing would need to be set out clearly".*

The government's proposals set out broad types of processing, such as processing for "business innovation purposes". However, the processing involved in "business innovation purposes" is likely to evolve and change over time. It is unclear what processing would be "necessary" for such purposes.

Nonetheless, for any processing on the list the balancing test would be removed and any processing in those circumstances will not be balanced against the interests of the individuals subject to that processing, even as that processing may evolve over time and endanger people's rights. This may lead to discriminatory outcomes where processing is used in unforeseen ways.

The government says that "the processing would still have to be necessary for the stated purposes and proportionate". However, necessity and proportionality tests do not provide sufficient protection to individuals without balancing the rights of individuals impacted. Furthermore, it is not clear how this proposal would interact with people's right to object to their data being processed. An organisation can only refuse a request if they have a compelling reason that overrides people's interests, rights and freedoms. As such, an organisation would need to conduct a balancing test at the point of objection, which could result in inconsistent outcomes and further compliance burdens for organisations.

In contrast, the current regime requires a balance to be conducted of the processing activity against the impact on individuals before the processing takes places. Legitimate interest is an exceptionally flexible ground in that it can be used for any reasonable purpose, provided the rights and freedoms of individuals are not overridden. The current approach is robust and flexible and can evolve to reflect different circumstances. It empowers organisations to think about the processing they intend to do and the impact on people at the outset and before being faced with objection requests from individuals. In turn, the balancing exercise helps organisations to consider wider issues such as safeguards, data minimisation, security, accountability and so on. This in turn results in less regulatory impact on organisations while simultaneously bolstering individual rights. Given the important safeguards they provide, ORG suggests that the Government should require organisations to make Legitimate Interest Assessments publicly available, not seek to remove them. Furthermore, as legitimate interest is an-oft misused lawful grounds for processing[9], ORG suggests that clearer and more affirmative guidance, as well as stronger enforcement, is needed from the ICO in this area.

[9] Bits f Freedom, *A Loophole in Data Processing*. Available at: https://www.bitsoffreedom.nl/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf

Issues with DCMS' rationale for proposals

The government's rationale for these proposals is based on a false premise that legal uncertainty is causing businesses to over-rely on consent, thus subjecting individuals to consent fatigue. The solution to consent fatigue is proper enforcement of consent which does not meet the GDPR thresholds for consent, not to amend the balancing exercise within the legitimate interests lawful basis. Otherwise, there is a risk that actors that are currently failing to meet the standards of consent that are required, could simply switch to legitimate interests to justify processing activities that result in real world harm, for example, in the AdTech field:

- Consumers have consistently expressed their preference not to consent or to opt-out to online tracking, direct marketing, or other privacy-invasive practices.[10]
- The data-driven industry relies on various manipulative and deceptive techniques, also known as dark patterns, which have been thoroughly documented and exposed.[11]
- Corporate lobbying has long opposed the introduction of legally binding signals, that would allow Internet users to set their privacy preferences once only, to opt out from being tracked by websites, and in a user-friendly manner, thus resolving consent fatigue and restoring consumers' agency.[12]
- Another example is Facebook's opposition to Apple's implementation of a feature that, similarly to legally binding signals, allows iOS users to set their preferences via software by answering a clear yes or no question.[13]

---

[10] Norwegian Consumer Council, *Out of Control*. Available at: https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/

[11] Norwegian Consumer Council, *Dark Patterns*. Available at: https://www.forbrukerradet.no/dark-patterns/

See also: Federal Trade Commission, *FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions*. Available at: https://www.ftc.gov/news-events/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap

[12] Corporate Europe Observatory, *Shutting down ePrivacy: lobby bandwagon targets Council*. Available at: https://corporateeurope.org/en/power-lobbies/2018/06/shutting-down-eprivacy-lobby-bandwagon-targets-council?hash=keZ3nidpfZbeVQAaYUYoSTDAvjXndSjmZurmIQLAQeY

[13] The Wall Street Journal, *Facebook Meets Apple in Clash of the Tech Titans—'We Need to Inflict Pain'*. Available at: https://www.wsj.com/articles/facebook-meets-apple-in-clash-of-the-tech-titanswe-need-to-inflict-pain-11613192406

Q1.4.2. To what extent do you agree with the suggested list of activities where the legitimate interests balancing test would not be required?

Strongly disagree

The introduction of any list is problematic. However, there are specific issues with the Government's proposed list of legitimate interests.

Firstly, it contains types of processing which are already covered by other legal grounds. For activities such as reporting of criminal acts or safeguarding concerns, there are existing lawful bases such as Article 6(1)(e) which permits processing which is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or processing is necessary for compliance with a legal obligation to which the controller is subject. These grounds should cover those activities. Similarly, "Delivering statutory public communications and public health and safety messages by non-public bodies" is easily justified "for the performance of a task carried out in the public interest" under Article 6(1)(e). It is unclear why there needs to be an additional legitimate interests ground. Thus, there appears no need to introduce legitimate interests as an alternative ground, particularly in the absence of the balancing test as a safeguard to guard against abuse of this ground.

Secondly, it contains types of processing which would already easily satisfy the balancing exercise. Thus, controllers should not have too much difficulty currently establishing a legal ground for their processing. For instance, many of other the activities, such as "Improving or reviewing an organisation's system or network security", "Improving the safety of a product or service that the organisation provides or delivers", or "Managing or maintaining a database to ensure that records of individuals are accurate and up to date, and to avoid unnecessary duplication" would pass the balancing test where controllers are engaging in basic activities. Thus, there does not appear to be a need to remove the balancing exercise when it can be readily satisfied by responsible controllers. On the other hand, removing the balancing exercise risks encouraging controllers to fit other, much less anodyne activities, within this lawful basis which risks abuse of the ground. This risk is exacerbated by the fact the list includes impossibly vague terms, for example, *"Using personal data for internal research and development purposes, or business innovation purposes aimed at improving services for customers"*. Indeed, these

purposes are so ill-defined that the Article 29 Working Party ('WP29') guidance on transparency cites similar phrases are cited as poor practices examples.[14] This could lead to overreliance by businesses on these grounds for a variety of processing.

ORG believes that it would be a risk to consider that processing for those purposes is always *prima facie* in the legitimate interests of controllers without any consideration of the impact on data subjects, as processing activities associated with that type of processing could range from the benign to harmful and may not always be confined to the types of processing which were originally envisaged by government / parliament. For example, "cookies or similar technologies" covers a wide range of processing activities, including processing that individuals are very concerned about. Consumer group Which? conducted studies that demonstrated the public concern with the use of such technology. Which? research found that:

> *"consumers care not just about what personal data is collected about them by online platforms for targeting adverts, but that how it is collected also matters. We find that consumers want greater transparency and control over how data is collected."*

Researchers also discovered that if consent over cookies was collected in a manner compliant with the UK GDPR, only a small fraction of consumers would agree to be tracked.[15] Legitimising such technology without any need to consider and balance the impact on individuals would thus be detrimental to consumers, while providing limited benefits for innovation.

Example of Impact

In October 2020, the ICO issued an enforcement notice against Experian, a data broking business.[16] Experian was reusing statutory credit reference data for marketing purposes in purported reliance on the lawful basis of legitimate interest. Addressing the issue of balancing tests, the ICO held that

> *"The Commissioner has explained in her own guidance that little weight can be attached to supposed benefit of the data subject consumer receiving direct marketing communications more*

[14] At page 9 https://ec.europa.eu/newsroom/article29/items/622227

[15] https://techcrunch.com/2019/08/10/most-eu-cookie-consent-notices-are-meaningless-or-manipulative-study-finds/

[16] ICO, *ICO takes enforcement action against Experian after data broking investigation*. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-takes-enforcement-action-against-experian-after-data-broking-investigation/

> *'appropriate' to them, when this is a consequence of processing and profiling to which they have not consented. The Commissioner considers that it is unlikely that a controller will be able to apply legitimate interests for intrusive profiling for direct marketing purposes."*[17]

For these reasons, the Commissioner concluded that the balancing test could not be considered properly or lawfully balanced, and Experian could not rely on legitimate interest as a lawful basis.

However, the Government are proposing to scrap the balancing test for activities such as *"Using personal data for internal research and development purposes, or business innovation purposes aimed at improving services for customers".* An irresponsible controller might consider that the "benefit of the data subject consumer receiving direct marketing communications more 'appropriate' to them" would mean this processing always falls within the category of processing aimed at improving customer services. The benefit of the balancing exercise conducted on a case by case basis to consider the impact on individuals would be lost. This would effectively legitimise this type of processing in the eyes of the organisation despite issues such as the lack of transparency, the intrusiveness of profiling, and the incompatibility with individuals' expectations over how their credit reference data is being used: factors which would otherwise fall to be considered as part of the balancing exercise and which should lead to the processing not being pursued because the interests of individuals would be seen to override that of the data controller.

[17] ICO, *Enforcement notice to Experian Limited*. Available at: https://ico.org.uk/media/action-weve-taken/enforcement-notices/2618467/experian-limited-enforcement-report.pdf

1.5 AI AND MACHINE LEARNING (1.5) *OR* REMOVING THE RIGHT TO HUMAN REVIEW)

Introduction

- The Government is considering the removal of Article 22 of the UK GDPR, which provides "the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects [...] or similarly significantly affects" individuals.
- ORG has concerns that as automation increases, important safeguards and protections for individuals are being hollowed out.
- ORG do not agree that the right should be removed. Instead, it should be strengthened by extending it to partly automated decision-making. The right to meaningful human involvement should also be clarified.

Response

Q1.5.14. To what extent do you agree with what the government is considering in relation to clarifying the limits and scope of what constitutes 'a decision based solely on automated processing' and 'produc[ing] legal effects concerning [a person] or similarly significant effects?

Strongly disagree

As automation takes an increasing role, safeguards against adverse effects should be strengthened. Removing the right a human review of automated decision-making is concerning given the trend towards the greater digitalisation of our society, with more and more decisions being made or helped by AI.

Article 22 does not apply to all automated decision-making but only where an organisation is carrying out decision-making solely by automated means, without any human involvement, where that decision-making has legal or similarly significant effects on them.

The burden on organisations when Article 22 arises is limited, requiring organisations to:

- give people information about the processing;
- introduce simple ways for them to request human intervention or challenge a decision; and
- carry out regular checks to make sure their systems are working as intended.

Thus, the right in Article 22 is currently of limited scope and application. Nonetheless, Article 22 of the UK GDPR has helped to provide remedies for individuals who were impacted by automated systems. For instance, Article 22 allows workers to stand up to abusive practices such as

- automated-firings:[18] the Amsterdam District Court has ordered Uber to reinstate six Uber drivers and pay compensation after they were unlawfully dismissed by algorithmic means, in a case that "is believed to be the first case of its kind brought under Article 22 of the EU General Data Protection Regulation (GDPR)"
- wage deduction:[19] Ola has been ordered to reveal information about profiling related to driver performance including the controversial driver 'fraud probability score' and 'earnings profile', both of which are used in an opaque manner in automated decisions regarding work allocation. In particular, "the court decided that a decision to make deductions from driver earnings amounted to an automated decision lacking human intervention. Such algorithmic decisions attract important legal protections according to Article 22 of the GDPR."

The right could however be extended to expand its protections and made flexible to ensure it is future-proofed. For example, the limit of the right to "legal" or similar effects is limiting in practice and could be usefully clarified through ICO guidance. Guidance could also address the extent of human involvement that is required. Article 22 could also be extended to partly automated decision-making to the phenomenon of automation bias, i.e. human actors placing excessive trust in decisions made by a machine. [20]

---

[18] ADCU, *Dutch & UK courts order Uber to reinstate 'robo-fired' drivers and pay compensation*. Available at: https://www.adcu.org.uk/news-posts/uber-to-reinstate-robo-fired-drivers-and-pay-compensation

[19] ADCU, *Gig economy workers score historic digital rights victory against Uber and Ola Cabs*. Available at: https://www.adcu.org.uk/news-posts/gig-economy-workers-score-historic-digital-rights-victory-against-uber-and-ola-cabs

[20] According to Jennifer Cobbe of Cambridge University, there exists a "*… well-attested psychological phenomenon of automation bias, which means that humans are more likely to trust decisions made by machines than by other*

CHAPTER 2

REDUCING BURDENS ON BUSINESSES AND DELIVERING BETTER OUTCOMES FOR PEOPLE

(*OR* REDUCING TRANSPARENCY AND ACCOUNTABILITY)

people and less likely to exercise meaningful review of or identify problems with automated decisions." Jennifer Cobbe, "Administrative law and the machines of government: judicial review of automated public-sector decision-making", Legal Studies (2019), 1-20.

2.2 REFORM OF THE ACCOUNTABILITY FRAMEWORK (*OR* SCRAPPING THE ACCOUNTABILITY FRAMEWORK)

Introduction

- The Government is proposing to revise the UK GDPR accountability framework, including a new approach based on privacy management operation programmes (PMPs). There are also proposals to remove the requirement to conduct a data protection impact assessment (DPIA).
- ORG has concerns that replacing the accountability framework with PMPs, and removing the DPIA duty, will undermine accountability and the GDPR's risk-based approach.
- ORG considers it essential that accountability requirements on controllers are not liberalised. It is imperative to preserve the DPIA duty, in particular.

Response

Q2.2.1. To what extent do you agree with the following statement: 'The accountability framework as set out in current legislation should i) feature fewer prescriptive requirements, ii) be more flexible, and iii) be more risk-based'?

Strongly disagree

The UK GDPR is already flexible and risk-based.

Organisations (Controllers) are required to "implement appropriate technical and organisational measures to ensure and to" demonstrate accountability. These measures must be proportionate to "the nature, scope, context and purposes of processing". These means that

- Encryption, pseudonymisation, and other security measures (Article 32 of the UK GDPR).
- Data protection policies (Article 25(2) of the UK GDPR).
- Contractual safeguards for Controller-Processor relationships (Article 28(3) of the UK GDPR).
- Records (Article 30 of the UK GDPR).

are all measures that can be implemented or not, according to the specific circumstances of the case. In particular, organisations that have less than 250 employees are not required to keep Records.

There are a number of tasks that organisations (Controllers) must carry out only if there is if a certain risk threshold is met. These requirements include:

- Data breaches need to be notified to the ICO only if they present a risk to the rights and freedoms of the individuals concerned (Article 33 of the UK GDPR). Individuals must be informed only when the data breach is likely to result in a high risk for his or her rights and freedom (Article 34 of the UK GDPR).
- Data Protection Impact Assessments must only be carried out for high-risk activities (Article 35 of the UK GDPR).
- Prior consultation with the ICO is required only if the activity is high risk and adequate measures to mitigate that risk were not identified after conducting the DPIA (Article 36 of the UK GDPR).
- The appointment of a Data Protection Officer is needed only for organisations that are public bodies or authorities, or if its core activities involve processing of sensitive data on a large scale or involve large scale, regular and systematic monitoring of individuals. Small organisations (employing <250 persons) only need to keep records in limited circumstances, , i.e., unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.(Article 30(5) of the UK GDPR.

Other obligations under the UK GDPR are also influenced by the level of risk involved, as higher risk will demand stronger technical and organisational measures, including security that is at a level appropriate to the risks presented by its processing.

Where the risk-threshold is met, the UK GDPR is prescriptive and sets out clear obligations which promotes legal certainty, including when it comes to enforcement. Organisations must be both accountable and able to demonstrate accountability to individuals or supervisory authorities. Contrary to the Government view at §139, prescriptiveness does not need to equate to a "box-ticking" exercise. For example, conducting a DPIA is not just an accountability but also serves as an early warning system for organisations against risks that may arise from processing

which will need to be mitigated. However, the consultation misconstrues DPIAs as an accountability measure only.

Q2.2.2. To what extent do you agree with the following statement: 'Organisations will benefit from being required to develop and implement a risk-based privacy management programme'?

Strongly disagree

Replacing the current accountability framework with "privacy management operation programmes" will introduce significant legal uncertainty, not lessen it. Responsible businesses benefit from existing accountability rules in that they are not only risk-based and proportionate, but also prescriptive. This provides them with clear requirements to fulfil. The proposals contain activities that would be part of PMOP which roughly overlap with existing accountability requirements. For instance,

- Instead of Data Protection Officers, organisations would be expected to designate individuals who are responsible for "overseeing the organisation's data protection compliance" and "representing the organisation to the ICO and data subjects".
- Instead of Records, organisations would be expected to produce "Personal data inventories".
- Instead of Data Protection Impact Assessments, organisations would be expected to produce "Risk assessment tools for the identification, assessment and mitigation of privacy risks across the organisation".

Thus, responsible businesses would perform similar activities to those set out under the current framework. However, the regulatory certainty provided by the legal framework, such as regarding the qualities and the independence requirements for the "designated individual", the kind of information that needs to be included in personal data inventories, and when and how to assess risks, would be absent. Conversely, there is a risk that irresponsible organisations would be able to exploit that same uncertainty to avoid complying with the rules.

Q2.2.3. To what extent do you agree with the following statement: 'Individuals (i.e. data subjects) will benefit from organisations being required to implement a risk-based privacy management programme'?

Strongly disagree

The existing accountability regime sets out clear obligations which promotes legal certainty, including when it comes to enforcement. Organisations must be both accountable and able to demonstrate accountability to individuals or supervisory authorities. However, it is not clear how the approach to accountability proposed by the DCMS will be enforceable, particularly by individuals.

On the contrary, individuals will lose legal tools that have proven invaluable to hold offenders to account and obtain remedies against the violation of their rights. For example, existing accountability requirements under the UK GDPR played a significant role in allowing individuals to enforce their rights against offenders. For instance:

- An ICO investigation into the NHS Free Trust and Google DeepMind found several shortcomings in how personal data of patients was handled, including that patients were not adequately informed that their data would be used as part of the testing programme for medical software developed by the companies. Inter alia, there was a failure to conduct a DPIA before commencing the project, which would have allow the companies to have assessed and appropriately mitigated the risks arising from the data processing. In this regard, the ICO stated: *"I am also concerned to note that the processing of such a large volume of records containing sensitive health data was not subject to a full privacy impact assessment ahead of the project's commencement"*[21] A legal challenge has now been issued on behalf of the 1.6 million individuals whose data was used as part of the testing programme.[22]

[21] ICO, *Royal Free - Google DeepMind trial failed to comply with data protection law*. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/

[22] The Register, *Brit law firm files suit against Google and Deepmind over use of hospital patients' data*. Available at: https://www.theregister.com/2021/09/30/royal_free_deepmind_representative_action_uk/

- A challenge to the South Wale's Police's use of live facial recognition[23] succeeded, in part, because there was a failure to properly conduct a DPIA which assessed the risks to the rights and freedoms of individuals and to mitigate these risks.
- The first DPIA of the NHSX Contact Tracing App exposed serious security and privacy flaws.[24] This contributed to a public discourse about digital contact tracing that culminated with the Government decision to abandon their original plans and develop a more privacy-preserving digital contact tracing system in its stead[25]
- The Test and Trace system, see also further below, was deployed without a DPIA, despite a DPIA being required before the system was deployed.[26] If carried out, the proposal to retain people's health data for 20 years is likely to have been flagged as excessive and unjustified, before the system was deployed. The retention period was subsequently changed to 8 years following an intervention from ORG. A DPIA may have prevented incidents such as data breaches,[27] distribution of sensitive information via social media channels by staff,[28] or sexual harassment perpetrated by bartenders with contact tracing details of their customers.[29]

---

[23] Liberty, *Liberty wins ground-breaking victory against facial recognition tech*. Available at: https://www.libertyhumanrights.org.uk/issue/liberty-wins-ground-breaking-victory-against-facial-recognition-tech/

[24] Michael Veale, *Analysis of the NHSX Contact Tracing App 'Isle of Wight' Data Protection Impact Assessment*. Available at: https://osf.io/preprints/lawarxiv/6fvgh

[25] BBC, *UK virus-tracing app switches to Apple-Google model*. Available at: https://www.bbc.com/news/technology-53095336

[26] BBC, *Coronavirus: England's test and trace programme 'breaks GDPR data law'*. Available at: https://www.bbc.com/news/technology-53466471

[27] BBC, *Coronavirus: Serco apologises for sharing contact tracers' email addresses*. Available at: https://www.bbc.com/news/uk-52732818

DigitalHealth, *Welsh data breach exposes information of Covid-19 patients.* Available at: https://www.digitalhealth.net/2020/09/public-health-wales-data-breach-covid-19/

The Guardian, *NHS Covid jab booking site leaks people's vaccine status*. Available at: https://www.theguardian.com/world/2021/may/06/nhs-covid-jab-booking-site-leaks-peoples-vaccine-status

[28] The Times, *Coronavirus contact tracers sharing patients' data on WhatsApp and Facebook.* Available at: https://www.thetimes.co.uk/article/coronavirus-contact-tracers-sharing-patients-data-on-whatsapp-and-facebook-rg3zqn5l6

[29] The Telegraph, *Test and trace is being used to harass women – already.* Available at: https://www.telegraph.co.uk/women/life/test-trace-used-harass-women-already/

Q2.2.7. To what extent do you agree with the following statement: 'Under the current legislation, data protection impact assessment requirements are helpful in the identification and minimisation of data protection risks to a project'?

Strongly agree

DPIAs help to identify potential negative consequences of processing operations early on in order to mitigate the impact of the potential risks. Indeed, the consultation notes that DPIAs can act as a mitigation against harms and as a barrier against some of the riskier reforms proposed by the consultation.

Considering the development of DPIAs helps to understand their utility. The Data Protection Directive ('DPD'), the precursor to the GDPR, did not require DPIAs. The DPD contained a series of notification and prior checking procedures which were complicated and placed burdens on Supervisory Authorities such as the ICO. The WP29 concluded that the notification system was 'not a useful or appropriate tool to provide information and transparency'. To solve these issues, the UK GDPR introduces requirements for DPIAs, which are described as 'effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes' (recital 89 UK GDPR). This balance seeks to facilitate data processing while mitigating risk, and assessments are only required where the processing may result in a high risk. Thus, DPIAs should not be viewed as a barrier to innovation. Instead they act as a filter to consider and alleviate the negative impacts that arise from high-risk processing. The consultation's proposals risk reverting to the unsatisfactory situation in the DPD.

Q.2.2.8. To what extent do you agree with the proposal to remove the requirement for organisations to undertake data protection impact assessments?

Strongly disagree

Removing the requirement to undertake DPIAs will result in increased uncertainty and wider, serious, and unmitigated impacts on individuals. This will result in increased dependence on the ICO. This would run contrary to the government's objectives and impede innovation.

Moreover, it is essential to consider the bigger picture and how the proposals operate cumulatively. The proposals are frequently inconsistent. For example, the consultation points to DPIAs as a necessary tool for the wider data protection regime, particularly as a safeguard in the context of amending the rules on international transfers. This demonstrates the problems that arise from removing the need to conduct DPIAs entirely.

During the coronavirus pandemic, the DPIA duty has been instrumental in ensuring that public actors conducted processing of public health data in a lawful manner. For instance, when the **Test and Trace** system became operational, there were concerns about (i) the fact that data would be stored for 20 years and (ii) the revelation that no DPIA had been conducted for the system, despite the law being clear that this is required prior to the processing of personal data.

A legal opinion on tech responses to the pandemic had previously concluded:[30]

> *We are of the view that … transparency would be best achieved through a Data Protection Impact Assessment that is made widely and publicly available, with appropriate views from the ICO on that DPIA also made public. Article 35 GDPR provides that, where a type of processing is "likely to result in a high risk to the rights and freedoms of individuals", the controller must carry out a DPIA. We note the ICO's "Examples of processing 'likely to result in high risk'" include "Innovative technology" and "Tracking". Further, Article 36 GDPR requires that the controller must consult the supervisory authority prior to processing where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. Our view is that any proposed measure for contact tracing is likely to result in high risk to the rights and freedoms of individuals, particularly considering the use of new technologies that involve tracking. We consider that these technologies must be the subject of a DPIA and consultation with the ICO prior to the processing of personal data.*

ORG instructed AWO solicitors to write to the Department of Health and Social Care (DHSC) about its concerns. Concessions were obtained on the retention period, a reduction to 8 years from 20. Finally, following a pre-action letter, DHSC admitted that a DPIA had not been conducted for the Test & Trace Programme as a whole and the programme had, therefore, been deployed unlawfully:

[30] Matthew Ryder QC, Edward Craven, Gayatri Sarathy & Ravi Naik (AWO), COVID-19 & Tech responses: Legal opinion, para 40, p. 16. Available at: https://www.awo.agency/covid-19-legal-opinion.pdf

> *"[t]he defendant accepts that: (i) Articule 35 applies to the Programme in its entirety; (ii) at or prior to the commencement of the Programme on 28 May 2020, there was not already in place a DPIA or DPIAs which addressed the processing of personal data across all aspects of the Programme; (iii) such a DPIA was and is required;"*

A failure to conduct a DPIA is more than a procedural failure. Conducting a DPIA is vital to understanding the problems that may arise about a system, in advance, and to ensuring public trust that their health data is being handled lawfully. In this case, Test & Trace was the main system to support the UK's capacity to test the spread of coronavirus. Ensuring trust and confidence in the way such a system uses personal data was essential to achieving the high levels of public participation needed to make the system a success.

Rather than removing the DPIA duty, ORG suggests that public actors should be obliged to make their DPIAs public to enhance transparency regarding public decision-making.

2.3 SUBJECT ACCESS REQUESTS (*OR* RESTRICTING THE RIGHT OF ACCESS TO PERSONAL DATA)

Introduction

- The Government plan to make it easier for organisations to deny subject access request based on the motives of the individuals who submit these requests. Furthermore, they are proposing to introduce a fee regime so that individuals would need to pay to exercise their right to access to their personal data.
- Subject access requests grant people transparency and access to their information. This access is often key to exercising other rights. Diluting the access regime and making it more difficult to people to access their data could dissuade individuals from exercising their rights and reduce transparency and accountability on the part of organisations.
- The SAR regime should remain free of charge. There is no evidence to justify changes to existing grounds for refusing SARs.

Response

Q2.3.1. Please share your views on the extent to which organisations find subject access requests time-consuming or costly to process.

The European Commission recently reviewed the EU data protection framework's impact and found no evidence of the right of access being too burdensome or costly for organisations. On the contrary, evidence shows that removing barriers to the right of access empowered individuals to control their data.[31]

Organisational capacity to process requests will be driven mainly by the amount of data which an organisation handles. An organisation which processes a lot of data should invest in ensuring it has the appropriate resources to respond to SARs in a timely and cost-efficient manner. Organisations should also collect the minimum amount of data necessary to accomplish their tasks, according to the principles of data minimisation and privacy by design and by default. If an organisation's capacity to handle requests becomes a consideration, this may encourage

[31] COM(2020) 264 final, *Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*. Available at: https://ec.europa.eu/info/sites/default/files/1_en_act_part1_v6_1.pdf

controllers to gather as much data as possible in order to reduce the burden to deal with access requests.

Q2.3.2. To what extent do you agree with the following statement: 'The 'manifestly unfounded' threshold to refuse a subject access request is too high'?

Strongly disagree

The threshold is intentionally high, to ensure access requests will not be unfairly rejected and to support the policy objective of access requests. The UK GDPR contains a nuanced set of principles that permit organisations to refuse access requests if they are abusive. The ICO's guidance clarifies the circumstances where the current threshold can be met. The current access request regime already allows organisations to refuse a request if it is malicious or if the access request is being used to harass the organisation and cause disruption.[32] The ICO gives clear guidance to organisation about how to apply the test. The current test strikes an appropriate balance between addressing the concerns of abusive requests, while ensuring individuals can know what data is being processed about them and thereby facilitating other rights.

Changes would result in greater uncertainty for controllers, reduce transparency and disempower individuals. There is no reliable evidence that the threshold is exposing responsible organisations to vexatious requests. On the contrary, a review run by the European Commission in 2020 found that removing barriers to the right to access has proven to empower individuals to control their data.[33]

[32] ICO, *When can we refuse to comply with a request?* Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/when-can-we-refuse-to-comply-with-a-request/#refuse2

[33] COM(2020) 264 final, *Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*. Available at: https://ec.europa.eu/info/sites/default/files/1_en_act_part1_v6_1.pdf

Q2.3.3. To what extent do you agree that introducing a cost limit and amending the threshold for response, akin to the Freedom of Information regime (detailed in the section on subject access requests), would help to alleviate potential costs (time and resource) in responding to these requests?

Strongly disagree

The FOIA regime serves a different purpose to the SAR regime. While the FOIA regime is designed to provide "public access to information held by public authorities", the SAR regime ensures that individuals are informed their data is being processed and that they have a right to access that information.

1. *Costs limit*

The introduction of any fee regime may result in those most reliant on the access regime, including vulnerable groups such as migrants, from being unable to access their rights. The right of access should not be an economic decision that individuals have to make. Introducing a costs limit could also provide controllers with an incentive to gather as much data as possible to reduce the burden to deal with access requests, as organisations could refuse requests on the basis that complying with them would exceed the cost limit. In other words, if you are inefficient enough to reach the cost limit when answering SARs, you are rewarded by being relieved from the obligation to answer such requests.

2. *Threshold*

The consultation proposes to introduce a vexatious test in the data protection regime based on the test in the FOIA regime. However, as discussed, the FOIA and SAR regimes go to different ends and serve different purposes, with the latter designed to inform individuals that their data is being processed and ensuring that they have a right to access that information. It is inappropriate for the government to compare the two regimes.

The test in the FOIA regime is whether the test is likely to 'cause a disproportionate or unjustifiable level of distress, disruption or irritation'. This permits an organisation to take into account the context and history of a request, including the identity of the requester and any previous contact with them. The government proposes that "applying similar provisions to subject access requests,..., would help to prevent organisations needing to respond to subject access requests where access to personal data or concerns about its processing are not the purpose of the request."

The proposed threshold test would allow controllers to request information concerning the purpose of a request, which will result in individuals not feeling able to exercise their rights. Moreover, the proposed threshold test would enable organisations to narrow the scope of a request. This would prevent individuals from being able to exercise their wider rights. The access request made in the context of the data protection regime will often be considered vexatious by its nature, because it is designed to empower individuals against controllers of their information by informing them what the data the organisation holds on them and how it is being processing. Individuals are likely to have a range of motives to making a request. It would not be beneficial for controllers to be able to refuse requests more easily based on the purpose of the request. In fact, this would hollow out the right of access.

In sum, such changes would disempower individuals and reduce accountability for controllers.

Q2.3.4. To what extent do you agree with the following statement: 'There is a case for re-introducing a small nominal fee for processing subject access requests (akin to the approach in the Data Protection Act 1998)'?

Strongly disagree

The impact assessment that accompanied the proposal for a General Data Protection regulation found that "In some Member States, data controllers are allowed to demand a fee to access their data". It continues by stressing that "individuals that asked data controllers for access to the data stored about them [...] received no or unsatisfactory responses". Together with other shortcomings, nominal fees were contributing "to individuals' perception that their rights are not effectively guaranteed.[34]Thus, the provision that "actions in response to the data subject's requests should be in principle free of charge" was enshrined in the GDPR.

Introducing a fee regime would have a chilling effect on individuals and their rights, particularly the vulnerable and disenfranchised.

[34] SEC(2012) 72 final COMMISSION STAFF WORKING PAPER, *Impact Assessment, Accompanying the document. Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) etc*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0072

The examples below illustrate how SARs have been used and highlights the impact that introducing nominal fees might have:

- Uber drivers have been using subject access requests to gather evidence of unfair dismissals[35] or racist accusations of fraud.[36]
- Workers at Olà, a gig-economy company, have been using subject access requests to uncover wage thefts.[37]
- Gambling companies have been profiling problem gamblers, using this information to fuel their addiction and hook them on gambling apps. Victims have been using subject access requests to unveil these predatory practices.[38]
- Public interest organisations have been using subject access requests to hold organisations to account and expose malpractices.
- Journalists have been using subject access requests to conduct investigations.

At §188, the government recognises that the proposal may impact persons less able to express themselves due to age or disability by resulting in their requests being erroneously treated as 'disproportionate' or 'vexatious'. The government suggests this may be mitigated by the fact that a third party can raise a subject access request on their behalf.

ORG submits this would be disempowering and inappropriately undermine a person's agency and ability to access their own personal data. This is unjustified in circumstances where there is no evidence supporting the introduction of a fee regime.

---

35 ADCU, *Dutch & UK courts order Uber to reinstate 'robo-fired' drivers and pay compensation*. Available at: https://www.adcu.org.uk/news-posts/uber-to-reinstate-robo-fired-drivers-and-pay-compensation

36 ADCU, *ADCU initiates legal action against Uber's workplace use of racially discriminatory facial recognition systems*. Available at: https://www.adcu.org.uk/news-posts/adcu-initiates-legal-action-against-ubers-workplace-use-of-racially-discriminatory-facial-recognition-systems

37 ADCU, *Gig economy workers score historic digital rights victory against Uber and Ola Cabs*. Available at: https://www.adcu.org.uk/news-posts/gig-economy-workers-score-historic-digital-rights-victory-against-uber-and-ola-cabs

38 The New York Times, *What a Gambling App Knows About You*. Available at: https://www.nytimes.com/2021/03/24/technology/gambling-apps-tracking-sky-bet.html

2.4 PRIVACY AND ELECTRONIC COMMUNICATIONS (*OR* SURRENDERING OUR RIGHT TO PRIVACY IN ELECTRONIC COMMUNICATIONS)

Introduction

- The consultation proposes reforms to the PECR, including relaxing the requirement for consent for cookies.
- ORG's has concerns that this technology can result in real-world harm. There has been legal action in Europe and the UK regarding the Adtech industry which exposes the harm that can be caused to individuals by the kinds of technologies discussed in the consultation. However, the consultation fails to take note of these developments.
- There is a need for stronger enforcement of existing norms in this area. It is essential that the consultation works in line with broader developments surrounding the regulation of the Adtech industry.

Response

This section of the consultation is concerned with, among other things, the use of behavioural advertising technology to "deliver personalised advertising and inform spending decisions of advertisers". While promoting the benefits of behavioural advertising technology, it fails to consider that the same technology can result in real-world harms.

The Irish Council for Civil Liberties ('ICCL') has conducted extensive research on the harms caused by behavioural advertising technology.[39] Judicial and regulatory action has been taken throughout Europe following the ICCL's research. In the UK, Jim Killock of ORG and Dr Michael Veale submitted a complaint to the ICO in 2018 regarding the failure of the AdTech industry to comply with the GDPR and UK Data Protection Act.[40]

The ICO has responded to those complaints by producing a detailed report into the industry.[41] That report found that "the current consent requests provided under both

[39] See https://www.iccl.ie/rtb-june-2021/

[40] The matter is currently the subject of an appeal to the Upper Tribunal (*Killock & Veale v the Information Commissioner*). The Upper Tribunal is considering the legality of the ICO's decision to close the complaint without providing the complainants with a substantive outcome.

[41] https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf

the TCF and AB frameworks are non-compliant" with the UK GDPR. The lead supervisory authority for such consent frameworks, the Belgian Data Protection Authority, has recently ruled that the IAB's consent framework is unlawful and must be amended.[42] Thus, it is likely that the frameworks which led to consent pop-ups, if not removed altogether, will be at least be amended. Rather than legitimising harmful conduct, the government's consultation should follow these regulatory developments.

Furthermore, there is currently an absence of technical controls in the Real-time bidding ('RTB') processing chain. This resulted in the "largest data breach ever recorded".[43] In the current system, a wide range of companies are permitted to collect data on individuals without any intention of providing adverts, only to sell individuals' profiles to third-party actors. The French supervisory authority ('CNIL') took enforcement action against several small AdTech companies, finding that the consent mechanisms they relied on were unlawful. According to CNIL, the companies did not and could not provide individuals sufficient information or control,[44] despite collecting vast amounts of data on individuals. At the time of the investigation, one company, Vectuary, had collected data on 67.6 million users from more than 32,000 apps.

According to research by *Which?*, consumers "care not just about what personal data is collected about them by online platforms for targeting adverts, but that how it is collected also matters. We find that consumers want greater transparency and control over how data is collected." Further research demonstrates that "when unacceptable, third-party sharing had occurred, concerns about privacy outweighed people's appreciation for ad personalization."[45]

Indeed, the industry is working on alternative mechanisms as it recognises that current forms of behavioural advertising are not working and fail to respect user control or choice.[46] Thus, the proposals in the consultation overlook industry trends and regulatory measures already taken to end such behavioural advertising practices.***Q2.4.1. What types of data collection or other processing activities by cookies and other similar technologies should fall under the definition of 'analytics'?***

[42] https://iabeurope.eu/all-news/update-on-the-belgian-data-protection-authoritys-investigation-of-iab-europe/

[43] See, https://news.sky.com/story/data-watchdog-slammed-for-lack-of-action-against-google-on-uks-largest-ever-data-breach-11910786; https://brave.com/rtb-evidence/;

[44] https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000037594451/

[45] https://hbr.org/2018/01/ads-that-dont-overstep

[46] https://ico.org.uk/about-the-ico/news-and-events/blog-adtech-the-reform-of-real-time-bidding-has-started/

"Analytics" in the context of the processing of personal data means the monitoring and analysis of behaviour to profile individuals. Thus, even the most anodyne analytical technology may cause real world harm.

Furthermore, a fixed definition of "analytics" would not be able to keep pace with the increased sophistication in analytical technology. As such, defining "analytics" would corrode individual choice and result in a regressive digital landscape in the UK.

Q2.4.2 To what extent do you agree with the proposal to remove the consent requirement for analytics cookies and other similar technologies covered by Regulation 6 of PECR?

Strongly disagree

A number of organisations[47] and academics[48] have found that the use of such technology has the potential to lead to harms. At a time when the industry itself has recognised the need for change, removing individuals' choice will perpetuate and engrain those harms. The proposed reforms would be retrograde and inconsistent with the government's commitment to end online harms. If enacted, the UK would become an outlier and an experiment ground for such technology and profiling.

Moreover, if consent was removed such technology would risk the safety of vulnerable groups and children. Vulnerable people cannot be siloed from such practices given the speed and scale of RTB. The proposed reforms will remove their agency to make decisions about how their data is used. Vulnerable groups and children should be given more agency over such technology, not less.

[47] See, inter alia, https://privacyinternational.org/learn/adtech; https://www.openrightsgroup.org/campaign/ending-adtech-abuse/; https://www.amnesty.org/en/documents/pol30/1404/2019/en/

[48] See, inter alia, https://www.forbes.com/sites/augustinefou/2021/01/03/digital-advertisingharms-society-heres-how/

Q2.4.3 To what extent do you agree with what the government is considering in relation to removing consent requirements in a wider range of circumstances? Such circumstances might include, for example, those in which the controller can demonstrate a legitimate interest for processing the data, such as for the purposes of detecting technical faults or enabling use of video or other enhanced functionality on websites?

Strongly disagree

The proposed reforms are unnecessary; they are contrary to developments in the use of such technology; and they will lead to real-world harms.

The specific details of the proposed reforms are likewise problematic. In order to ensure that the use of such technology always has a lawful basis, the reforms suggest eliminating the balancing test and instead relying on legitimate interests. If the balancing test is removed, the risk to individuals will not be considered in circumstances where there are well-documented risks. This will result in a proliferation of behavioural profiling with severe consequences for individuals. The proposed reforms are therefore inconsistent with the government's position on online harms and would lead to a proliferation of online and real-world harms.

Q2.4.4. To what extent do you agree that the requirement for prior consent should be removed for all types of cookies?

Strongly disagree

Cookies enable widespread and uncontrolled surveillance and behavioural profiling of individuals, which have resulted in real-world harms. For instance, gambling operators are able to use cookies to profile and target vulnerable individuals with gambling addictions. Likewise, research from the ICCL has shown that people can be micro-targeted on sensitive and intimate personal details through the use of cookies, for example through codes that denote someone as "Christian".

This reform would be facilitate and legitimatise some of the most harmful practices online, leading to adverse consequences for British citizens at a time where the UK government seeks to embark on a world-leading online harms agenda.

Q2.4.5. Could sectoral codes (see Article 40 of the UK GDPR) or regulatory guidance be helpful in setting out the circumstances in which information can be access on, or saved to a user's terminal equipment?

ORG would welcome a sectoral code with the objective of clarifying and narrowing the scope of what is strictly necessary. However, ORG does not support the development any code or guidance that seeks to legitimise current industry practices.

Q2.4.8. What, if any, other measures would help solve the issues outlined in this section?

The enforcement of existing norms would (i) protect individuals and (ii) end consent pop-ups. Cookie pop-ups arose as a veneer to seeking consent. However, consent pop-ups do not appropriately serve that purpose, as demonstrated by enforcement actions by supervisory authorities, including the ICO. Greater enforcement would end unlawful behavioural cookies and normalise the use of functional cookies only. Indeed, the technology that powers behavioural advertising, Real-Time-Bidding, is irreconcilable with any reasonable data protection standard.

2.5 USE OF PERSONAL DATA FOR THE PURPOSES OF DEMOCRATIC ENGAGEMENT (*OR* ABUSING PERSONAL DATA UNDER THE GUISE OF DEMOCRATIC ENGAGEMENT)

Introduction

- The proposals are querying if the lawful grounds for processing for the purposes of democratic engagement impede the use of data and need to be expanded
- ORG has concerns that the lawful grounds for processing are already very expansive and political parties are permitted to interpret them in an extremely broad manner. To increase the grounds further would be unnecessary.
- There is no reason to increase the grounds further. On the contrary, there is a current issue regarding the expansive nature of how political parties interpret the necessity requirement for the processing of data revealing political opinions. There needs to be stronger enforcement from the ICO in this area.

Response

Q2.5.4. To what extent do you think the lawful grounds under Article 6 of the UK GDPR impede the use of personal data for the purposes of democratic engagement?

Strongly disagree

The DPA 2018 augmented the lawful grounds for processing under Article 6 UK GDPR to permit the use of personal data for democratic engagement. The expanded basis was brought into the DPA 2018, despite concerns raised by the ICO. A further expansion is unnecessary. This is explained in more detail below.

The use of data in the democratic process has been subject to reports and scrutiny from the ICO. The current position in the UK GDPR is that organisations involved in processing for the purposes of democratic engagement have a wider discretion for processing under §8(1)(e) of the DPA 2018 extends the concept of 'public interest' under Article 6(1)(e) GDPR to include 'an activity that supports or promotes democratic engagement'. This is – and is intended to be – a wide exemption. Margot James MP, the minister presenting the Data Protection Bill, as it then was, explained that the term was designed with the intention of covering 'a range of activities

carried out with a view to encouraging the general public to get involved in the exercise of their democratic rights' (Public Bill Committee, 2018). The Minister said it could include communicating with electors, campaigning activities, supporting candidates and elected representatives, casework, surveys and opinion gathering, and fundraising to support any of those activities. Any processing of personal data in connection with those activities would have to be necessary for their purpose and have a legal basis. The explanatory notes to the Act confirm that [t]he term 'democratic engagement' is intended to cover a wide range of political activities inside and outside election periods, including but not limited to: democratic representation; communicating with electors and interested parties; surveying and opinion gathering, campaigning activities; activities to increase voter turnout; supporting the work of elected representatives, prospective candidates and official candidates; and fundraising to support any of these activities. This provides a wide ground for processing personal data (albeit not special category data such as data about political opinions, regarding which, see below).

In turn, political consultancies and parties may rely on §8 DPA 2018 to process personal data without needing to engage with the data subject at all. This should assuage the consultations concerns about restrictions on their ability to reach voters, but at the same time it strips back one of the core protections of personal political data. During the passage of the Act, the ICO expressed concern about this extension of 'public interest', stating that the ICO

> *considers that consent or 'legitimate interests' under article 6 of the GDPR are the more appropriate lawful bases for such processing. The legitimate interest basis enables the balancing test of whether such interests are overridden by the interests or fundamental rights and freedoms of the data subject. This balancing test is important to ensure that some organisations do not use a broad legal basis to legitimise some of the campaigning techniques the Commissioner's office is looking at in her investigation into data analytics for political purposes.*
>
> *9. Having considered Recital 45 of the GDPR, the Commissioner considers that not all democratic activities would be covered by Article 6 (1) (e). It is likely to be restricted to activities such as those covered by electoral law, for example sending mail outs allowed to each voter. Unlike the democratic engagement, the other activities listed in Clause 8 do have a broad legal basis, for example if necessary for the exercise of a function conferred by enactment, functions of Parliament or the administration of justice.*

> *10. The very wide democratic engagement provision also contrasts with the processing of special category data (political opinions) in the relevant Article 9 legal basis in the Bill as drafted (and the current DPA 1998 Schedule 3 condition) which are only able to be used by registered political parties rather than by any data controller. Other campaigners or private sector organisations have to rely on consent unless, for example, electoral law allows them access to the full electoral register in advance of a referendum. (Information Commissioner's Office, 2018c)*

Accordingly, the DPA 2018 provides a "very wide democratic engagement provision" for such processing. That wider basis was introduced despite the concerns of the ICO. Nevertheless, the consultation proposes to expand that basis further.

Q2.5.5 To what extent do you think the provisions in paragraphs 22 and 23 of Schedule 1 to the DPA 2018 impede the use of sensitive data by political parties or elected representatives where necessary for the purposes of democratic engagement?

Strongly disagree

Paragraphs 22 and 23 Schedule 1 to the DPA 2018 provide a wide basis for political parties to process special category data. They only need to justify the processing as "necessary". Political parties have interpreted the necessity requirement broadly.[49] The ICO has not taken any enforcement action to stop them from processing special category data.

In sum, ORG submits that there is no reason to increase the grounds further. On the contrary, there is a live issue regarding the expansive nature of how political parties interpret the necessity requirement for the processing of data revealing political opinions. ORG considers that there needs to be stronger enforcement from the ICO in this area.

For instance, members of ORG filed complaints to the ICO about processing by the main political parties in England (the Labour, the Conservatives, and the Liberal Democrats).

These complaints were filed on the basis of information received from political parties in response to subject access requests which showed the profiling they were

[49] See, https://www.openrightsgroup.org/campaign/data-and-democracy-project/

subjected to, as well as subsequent interactions between ORG and the parties regarding their data processing.[50] The complaints also emerged against a backdrop of an ICO Audit Report which found that the parties engaged in extensive data gathering to profile voters and using the predictions to engage with voters to encourage them to vote and / or change their voting behaviour. The Information Commissioner also confirmed that *"it was illegal for the Conservative Party to collect and process "ethnicity data""*.[51]

ORG's complaints show how that the parties have not appropriately addressed their minds to these necessity and proportionality tests.[45] For instance, the response from the Labour Party suggested that any processing that assists them to win an election would be necessary:

> *"The Party…. does consider that all of its data processing is in the substantial public interest because it reasonably believes that this data processing contributes to the prospects of the election of Labour Party MPs who could implement the Party's policy platform."*

The converse of that argument would be that there is no limit to that processing. Thus, the complaint concluded that:

> *"the political parties are treating anything that helps them achieve their political goals – whether invasive profiling or not deploying sufficient resources to comply with subject access requests – as necessary or otherwise lawful."*

The ICO was asked to respond to the address the issues raised in the complaint. It might be assumed that the ICO would not allow unrestricted processing, in light of the ICO's own concerns about data processing by political parties. For instance, the ICO's audit of the political parties found that the "lawful bases that parties were processing personal data under were not always appropriate."[43] The ICO criticised the parties' application of §8 and Sch 1 DPA and found that where no appropriate legal basis can be found, such processing "must cease"[44].

However, to date, the ICO has failed to provide them with a substantive outcome to their complaint or to fully investigate the substance of their complaint. In relation to the instant question (Q2.5.5), this example illustrates that parties are already able to

[50] For example, Labour and the Conversatives purchased estimated data by geodemographic segmentation. The Conservatives purchased onomastic data, i.e. information derived from the study of people's names which identified a person's county of origin, ethnic origin and religion based on their first and last name.

[51] https://parliamentlive.tv/event/index/d4a948dd-b19a-4ece-adbe-8d84cfab09c5

process vast quantities of data with very little impediment from the regulation or regulator. Any reform would thus be unnecessary.

CHAPTER 3

BOOSTING TRADE AND REDUCING BARRIERS TO DATA FLOWS

(*OR* BOOSTING DATA LAUNDERING)

Introduction

- The Government propose to weaken the protections for personal data in international data transfers.
- ORG has concerns that liberalising how transfers can take place will negatively impact individuals' rights and freedoms and the protection of their personal data. The changes proposed could also risk imperilling the UK's adequacy decision as the UK risks becoming a conduit for data transfers from the EU to countries which offer lesser protections for individual's rights.
- The existing regime is already flexible and risk-based. It is not clear why the changes proposed are needed, particularly in light of the impact for individual's rights and the risk the proposals pose to the UK's adequacy decision.

Response

Q3.2.1. To what extent do you agree that the UK's future approach to adequacy decisions should be risk-based and focused on outcomes?

Strongly Disagree

The adequacy system ensures that an equivalent level of data protection is provided by another country, territory, sector or international organisation to the system within the UK. This is important to ensuring that people's data is protected when it is transferred to another country from the UK.

The current regime facilitates transfers in a range of circumstances. If there is an adequacy decision, data can be transferred on that basis. Where there is no adequacy decision, then transfers are only permitted provided that there are "appropriate safeguards" put in place to reflect the specific risk.

The current regime is already flexible and risk-based, i.e. the need to ensure *"appropriate* safeguards*"*, so it is not clear why a change is needed. Liberalising how transfers can take place could also risk losing the UK's own adequacy finding from the EU. The government state:

> *Adequacy assessments should take into account the likelihood and severity of actual risks to data subjects' data protection rights. This approach will account for the actual practices that materially affect international data transfers between the UK and another jurisdiction, rather than accounting for academic or immaterial risks. There may be practices in a particular country that are perceived to undermine data*

subject rights but if, for example, these practices are not applied in specific sectors or territories, then the risk to data subjects when making an adequacy finding in respect of those specific sectors or territories is very low or immaterial.

This statement is very vague. It is not clear how "actual risks" to data protection should be differentiated from "academic or immaterial risks". ORG considers that it is essential to retain a holistic assessment of the equivalence of the protection provided by a legal framework for data subject's rights.

Q3.2.2. To what extent do you agree that the government should consider making adequacy regulations for groups of countries, regions and multilateral frameworks?

Strongly Disagree

Groups of countries, regions and multilateral frameworks will have different approaches to safeguarding personal data. The risk will change from country to country, region to region, framework to framework. It follows the analysis concerning the level of protection afforded by such frameworks has to be done on a national basis to reflect the risk that is inherent in the transfer.

It is not clear why the Government should consider making adequacy decisions for groups of countries and regions. Geographic proximity does not guarantee any level of legal protection and legal frameworks will vary hugely between regions. If adequacy is granted for a region which contains countries that do not adequately protect personal data, then that would rid adequacy of its purpose, which is to only permit the transfer of data to countries which provide an *equivalent* level of data protection (or, if adequacy does not apply, to put appropriate safeguards in place).

Indeed, the Government mention the Council of Europe modernisation of Convention 108 on Data Protection as an example of a "multilateral framework". The Convention does provide, in principle, high standards of personal data protection. In practice, however, this will depend on several factors, such as whether a given country has implemented the Convention or only ratified it, and whether, based on an analysis of the provision of the Convention, the national legal frameworks and practices have to be changed and adhered to. If adequacy is granted for a framework that includes states or actors that don't ensure an appropriate level of protection for personal data this would undermine the adequacy regime.

Ultimately, a holistic consideration of the national data protection framework is the only reliable way to assess the risks in the destination of transfer and whether the personal data being processed in such country are afforded an equivalent level of protection or not. As discussed earlier, where there is no adequacy decision, the existing regime already provides for a flexible and risk-based approach permitting

transfers of data to a range of actors provided that appropriate safeguards are put in place.

Q3.2.4. To what extent do you agree that redress requirements for international data transfers may be satisfied by either administrative or judicial redress mechanisms, provided such mechanisms are effective?

Strongly Disagree

There is no guarantee that these redress systems would be equally effective and may depend on the circumstances of the case or the legal system in question. ORG considers it important to retain a holistic assessment of the equivalence of the protection provided by a legal framework for data subject's rights, including with respect to the relevant oversight mechanisms and redress avenues.

Q3.3.1. To what extent do you agree with the proposal to reinforce the importance of proportionality when assessing risks for alternative transfer mechanisms?

Strongly Disagree

Although addressing risk to data subjects rights can be challenging and time-consuming for organisations, it is essential to ensure an equivalent level of protection for the personal data of individuals whose data is being transferred out of the UK to another jurisdiction.

The existing regime already enshrines proportionality in that "appropriate safeguards" must be used when making transfers to a jurisdiction that is not covered by adequacy. It is not clear what further changes the government intends to make.

We are aware that the Information Commissioner's Office is committed to producing guidance and tools to enable organisations to comply with the law and continue to enable data flows. The recommendations that ORG formulated during that consultation would help address these challenges without negatively impacting the rights and freedom of individuals.[52]

[52] Open Rights Group, *Submission to the Information Commissioner's Office – International Transfers Under the UK GDPR*. Available at: https://www.openrightsgroup.org/publications/open-rights-group-submission-to-the-information-commissioners-office-international-transfers-under-the-uk-gdpr/

Q3.3.4. To what extent do you agree that empowering organisations to create or identify their own alternative transfer mechanisms that provide appropriate safeguards will address unnecessary limitations of the current set of alternative transfer mechanisms?

Strongly Disagree

Article 46(3)a of the UK GDPR already allows organisations to transfer personal data based on "contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation", provided that these contracts were approved by the Commissioner beforehand.

The government now proposes that organisations can create alternative transfer mechanisms (ATMs) without the need for approval by the ICO. This is likely to lead to a risk of inconsistent levels of protection. There would be increased uncertainty for organisations as to whether the ATMs provide appropriate safeguards. There would also be increased risks for individuals as the ATMs may not provide an appropriate level of protection for their rights.

Significantly, the proposal relies on organisations conducting their own impact assessments, which underscores the need to retain DPIAs contrary to the government's other proposals. The government also anticipates organisations could be supported by guidance. Allowing organisations to create their own contractual instruments without approval from the ICO is dangerous, particularly in respect of higher risk transfers, and could imperil the UK's adequacy decision.

Q3.3.7. To what extent do you agree that the proposal to create a new power for the Secretary of State to formally recognise new alternative transfer mechanisms would increase the flexibility of the UK's regime?

Strongly Disagree

It is more appropriate that these assessments be carried out by the ICO as an independent regulator, as provided for within the existing regime.

Furthermore, such a power would attract a significant amount of lobbying pressure from corporate entities that are interested in getting their own "transfer mechanism" approved, a situation that would further undermine the credibility of this function.

On the other hand, Article 46(3)a of the UK GDPR already allows organisations to transfer personal data based on their own contractual instruments, provided that the ICO approves these. Being an independent authority, the Commissioner is better

suited to make such considerations in an objective manner and resist external pressure.

Q3.4.1. To what extent do you agree with the approach the government is considering to allow certifications to be provided by different approaches to accountability, including privacy management programmes?

Strongly Disagree

Accountability is a fundamental principle of data protection. It is imperative that organisations are accountable and can in turn demonstrate that accountability to data subjects and supervisory authorities.

The issues with privacy management programmes have been discussed elsewhere in ORG's response, not least that they will lead to increased legal uncertainty on the part of organisations and thereby gaps in compliance. Basing international transfers on vaguely defined privacy management programmes would not adequately safeguard individuals' rights to have their personal data protected when it is transferred out of the UK.

Q3.5.1. To what extent do you agree that the proposal described in paragraph 270 represents a proportionate increase in flexibility that will benefit UK organisations without unduly undermining data protection standards?

Strongly Disagree

The government proposes establishing a proportionate increase in flexibility for the use of derogations by making it explicit that the repetitive use of derogations is permitted.

This would be a marked shift from the EU approach that treats derogations as exceptional. Derogations should not be used repetitively due to their exceptional nature and the inherent risks involved. As the ICO states:

> *Where transfers are repeated and predictable, there is an opportunity to put in place appropriate protections for people's data, through the use of an AITM. Where it is possible to put such protections in place, either wholly or in part, this should be done to ensure people are protected.*

However, the government's proposals would turn the exceptional into the norm. These changes would also risk jeopardising the adequacy decision. The EDPB has stressed that derogations cannot be relied on for regular and repetitive transfers.[53]

[53] European Data Protection Board, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*. Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

CHAPTER 5
REFORM OF THE INFORMATION COMMISSIONER'S OFFICE (*OR* UNDERMINING INDEPENDENT OVERSIGHT)

5.2 STRATEGY, OBJECTIVES AND DUTIES

Introduction

- The Government is proposing to introduce a new duty for the ICO to balance enforcement against economic interests. The Government is also asking to introduce a new power for the Secretary of State for DCMS to dictate strategic priorities to the ICO. Finally, the Government want to have the power to amend the salary of the Commissioner without Parliamentary approval.
- ORG considers these proposals to be fundamentally incompatible with the idea of effective, independent oversight.
- The ICO must remain independent so that it can uphold rights over personal data and operate independently of government.

Response

Q5.2.4. To what extent do you agree with the proposal to introduce a new duty for the ICO to have regard to economic growth and innovation when discharging its functions?

Strongly disagree

The ICO is an independent regulatory authority. Its independence is provided for in Article 52 UK GDPR which states that the Commissioner "shall act with complete independence in performing tasks and exercising powers in accordance with this Regulation." The proposed reforms threaten the independence of the ICO and its ability to uphold individuals' rights over personal data.

The scope of the proposed duty on the ICO to "have regard for economic growth and innovation when discharging its functions" is unclear. The ICO already considers "enabling innovation and growth" in the discharge of its duties.[53] Therefore, a further duty may be contrary to the Information Commissioner's function to independently uphold rights. At times, the complete and effective protection of data subjects may curtail economic growth in order to promote wider societal objectives.

[53] See Section 2 of the 2020 – 2021 report: https://ico.org.uk/media/about-the-ico/documents/2620166/hc-354-information-commissioners-ara-2020-21.pdf

For instance,

- Google[54] and the AdTech industry[55] have repeatedly reiterated that harmful online advertising surveillance is necessary for "financial sustainability".
- Facebook argued that enforcing the Schrems II judgement would have "devastating" and "irreversible" consequences on its business.[57]

Thus, requiring the ICO to "have regard" to growth and innovation may result in inconsistent and weaker protections for individuals, in cases where individual rights are seen to prevent innovation.

ORG also opposes any proposal "to oblige the ICO to undertake and publish impact assessments, as well as conduct enhanced consultation, when developing codes of practice, and complex or novel guidance" (Q5.5.1. to Q5.5.5).

Q5.2.11. To what extent do you agree with the proposal for the Secretary of State for DCMS to periodically prepare a statement of strategic priorities which the ICO must have regard to when discharging its functions?

Strongly disagree

This would undermine the independence of the Information Commissioner. Reforms that impact on the independence of the ICO may be inconsistent with Article 52 UK GDPR.

The Information Commissioner has noted the concern of the introduction of a statement of strategic priorities, stating that "it is critical that any SSP still enables the regulator to operate independently of government." The Information Commissioner suggests that Parliament set the ICO's objectives instead of government, to retain independence.

---

54 Euractiv, *Digital Brief, powered by Facebook: Microtargeting debate, Protecting gig workers, Apple antitrust*. Available at: https://www.euractiv.com/section/digital/news/digital-brief-powered-by-facebook-microtargeting-debate-protecting-gig-workers-apple-antitrust/

55 IAB Europe, *Open Letter on the Digital Services Act (DSA) and Digital Advertising*. Available at: https://iabeurope.eu/wp-content/uploads/2021/07/16th-July-2021-DSA-Digital-Advertising-Open-Letter-From-Industry-Players-Associations.pdf

57 Reuters, *Facebook faces prospect of 'devastating' data transfer ban after Irish ruling*. Available at: https://www.reuters.com/business/legal/facebook-data-transfer-ruling-irish-court-due-friday-2021-05-14/

The suggestion that the Secretary of State should prepare a statement of strategic priorities which the ICO "must have regard to when discharging its functions" will frustrate the capacity of the ICO to act independently.

5.3 GOVERNANCE MODEL AND LEADERSHIP

Q5.3.5. To what extent do you agree that the salary for the Information Commissioner (i.e. the proposed chair of the ICO in the future governance model) should not require Parliamentary approval?

Strongly disagree

Parliament should approve amendments to the ICO's salary, not government, to retain independence.

5.6 COMPLAINTS (*OR* RESTRICTING THE RIGHT TO COMPLAIN)

Introduction

- The Government proposes to increase the discretion with which the ICO can decide not to investigate a complaint
- There are existing issues with ICO enforcement including that the ICO already approaches complaints with a large degree of discretion. The proposals will lead to more uncertainty for individuals and adversely affect their rights to hold controllers to account.
- The ICO's discretion should not be further increased. The government could reconsider implementing Article 80(2) UK GDPR in light of recent developments in the *Lloyd v Google* case, that have further constrained the legal options for challenging data protection harms.

Response

Q5.6.1. To what extent do you agree that the ICO would benefit from a more proportionate regulatory approach to data protection complaints?

Q5.6.4. To what extent do you agree with the proposal to set out in legislation the criteria that the ICO can use to determine whether to pursue a complaint in order to provide clarity and enable the ICO to take a more risk-based and proportionate approach to complaints?

Strongly disagree

The right of an individual to seek effective remedies against a controller through the ICO is integral to ensuring the rights in the UK GDPR are effective. The proposed changes to the ICO's role would curtail the Information Commissioner's ability to uphold individuals' rights. Granting the Information Commissioner discretion to "decide not to investigate a complaint" would lead to uncertainty for individuals. Furthermore, it is not appropriate to measure enforcement by the "value" on the outcome, given that the importance to an individual receiving an outcome is inherent in the fact that a complaint has been made.

Moreover, any reforms must reflect the cautious approach and wide margin of discretion of the Information Commissioner to regulatory action. In particular, under

paras 165 – 166 DPA 2018, the Information Commissioner need not provide a complainant with enforcement action as an "outcome".

This discretion is the subject of an appeal to the Upper Tribunal in *Killock & Veale v the Information Commissioner*. The appellants, Jim Killock of ORG and Michael Veale, made a complaint to the ICO regarding the AdTech industry in September 2018, pursuant to section 165 of the Data Protection Act. In 2021, the ICO closed their complaint despite the fact that, to date, no substantive steps have been taken by the ICO to address the substance of their complaint which related to the industry's failure to comply with the GDPR and Data Protection Act 2018. The purported outcome in their case was that the ICO says it has investigated the matter "to the extent appropriate", and advised the complainants that their complaint has "assisted and informed the ICO's broader regulatory approach to RTB since September 2018". The appellants have appealed against the ICO's decision to close their complaints, without providing a substantive outcome, and judgment is awaited.

The Commissioner rarely takes enforcement action against data controllers even when widespread or systemic issues are highlighted. Instead, the Commissioner focuses on practices that may result in higher risks to individuals, such as in the data broker industry or the democratic process. This position can frustrate data subjects. The protection afforded to individual data subjects would be reduced if the Commissioner is granted further discretion.

Furthermore, legislating for "criteria that the ICO can use to determine whether to pursue a complaint" will lead to uncertainty as any such criteria will not be able to deal with the range of different issues that arise from data processing. Conversely, the current regime allows for a degree of predictability and foreseeability in what the Commissioner can and cannot do in response to a complaint. Introducing a proportionality test would introduce uncertainty and possibly inconsistent decision making.

Finally, the Government could reduce pressure on the ICO to handle individuals' complaints through reconsidering its February 2021 decision not to implement Article 80(2) GDPR. This would permit non-profit organisations to represent individuals *without* their authority before the ICO and in the courts and would be particularly useful for systemic-type breaches.

The DCMS decision was as follows:

> *"The government has considered the arguments for and against implementing Article 80(2) of the UK GDPR which would permit non-profit*

organisations to represent individuals without their authority. The current regime already offers strong protections for individuals, including vulnerable groups and children, and routes for redress. In the government's view, there is insufficient evidence of systemic failings in the current regime to warrant new opt-out proceedings in the courts for infringements of data protection legislation, or to conclude that any consequent benefits for data subjects would outweigh the potential impacts on businesses and other organisations, the ICO and the judicial system."

In reaching that decision, the DCMS referred to the *Lloyd v Google* case, which was (then) yet to be heard in the UK Supreme Court. The DCMS said that:

> *"Although cases brought under the civil procedure rules are different from claims brought under Article 80(2) of the UK GDPR because they rely on an affected individual to act as the lead claimant when representing the interests of others, they demonstrate the potential for a form of representative action to succeed under the existing Rules.* The government will continue to monitor developments in this area closely*"* (emphasis added).

As there has now been a judgment in *Lloyd v Google* case,[58] which held that the representative action brought by Mr Lloyd was not possible in the form it was brought, ORG suggests that DCMS should now reconsider whether the introduction of Article 80(2) GDPR is needed to ensure that data subjects have adequate access to justice for data protection breaches.

Q5.6.2. To what extent do you agree with the proposal to introduce a requirement for the complainant to attempt to resolve their complaint directly with the relevant data controller prior to lodging a complaint with the ICO (with guidance and exemptions)?

Strongly disagree

There is no reliable evidence about complaints being lodged in a vexatious manner or for reasons that could have easily been resolved by contacting the organisation subject to complaint. On the contrary, the ICO stress in their annual report that complainants usually contact the ICO only after having received unclear or untrustworthy information from the organisation they complain about.

[58] *Lloyd v Google LLC* [2021] UKSC 50

> *"when data controllers fail to fully explain to complainants how they have arrived at a decision, understandably the public turns to the regulator. [...]*
>
> *In around half of the cases that we looked at in 2019, we found that there was more the data controller could have done to either improve their information rights practices, or explain in a more comprehensive way how they are complying with their legal obligations. Consequently, this year we have asked data controllers to revisit concerns and do more to assure themselves and complainants that they are complying with their obligations under the law."*[59]

Introducing such a requirement would further dilute the right of the individual to complain. This could have a chilling effect and contains the potential to intimidate those who have less power, e.g. former employees, those with vulnerabilities. These people might be reasonably dissuaded from exercising their rights should they need to interact with the controller first.

Moreover, there are instances where the complexity and opaqueness of digital ecosystems make it difficult, if not impossible, to identify an organisation to complain against. For instance, in the case of Adtech, surveillance advertising practices are the result of a vast network of intermediaries, many of whom may be located outside of the GDPR's territorial reach (or, at least, will mount this as a defence). In such circumstances, complainants must retain a right to complain to the ICO.

[59] ICO, *Annual Report 2019-20*. Available at: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf