Data protection in post-Brexit Britain: A response to the Government of the United Kingdom's public consultation on reforms to the data protection regime (*"Data: A new direction"*)

by Wes Damen, Adam Harkens, Wenlong Li, Emma Ahmed-Rengers, and Karen Yeung

Birmingham (UK)
15 December 2021

Table of Contents

1. Introduction

I.

Ever since the United Kingdom's exit from the European Union, the UK government has made it clear that they see opportunities for enacting new legislation. One of these opportunities is to legislate how new technologies are to be used, and how citizens' personal data is handled where it is used as a necessary component of such technologies. On September 10th 2021, the Department for Digital, Culture, Media & Sport (DCMS) launched its public consultation for proposed reforms to the UK's data protection regime.[1] We believe that it is appropriate that careful eyes are kept on the UK's data protection regime in order to ensure that existing legal frameworks are appropriately future proofed, especially when we consider that the overall UK regulatory environment is in-flux, as UK law and policy begins to diverge from that of the European Union. This appropriate future proofing of a new data protection laws includes both the public and private sector use of technologies requiring the processing of high-volumes of personal data – in many cases making use of machine learning techniques – that can expose data subjects to considerable harms to their fundamental rights and personal interests. In this response we set out some of the concerns we are having about this legislative proposal, and why a change of course is called for.

II.

Considering the possibilities for reform set out by DCMS, the UK is now at a crossroads with regard to addressing the balance between **(a)** protection against potential dangers and risks produced by high-volume data collection, retention and processing of personal data (both for individuals and the public interest), and **(b)** the freedom and capacity to innovate. This raises and important question: does the UK government want to alter this balance as it currently stands?

The government can either:

1. Strengthen legal protections, while reducing the freedom to innovate at the cost to innovation of all kinds;
2. Weaken legal protections to enhance the freedom to innovate, at a cost to individuals and the public interest, with regard to the occurrence of various data harms that this may enable.
3. Maintain the current balance, but *improve upon* existing EU laws, where there are genuine opportunities to clarify and improve legal definitions, processes, and procedures.

The consultation document claims to increase both the freedom to innovate and the scope of said innovation, *and* maintain strong levels of data protection afforded to UK citizens. In other words, that we can have our cake and eat it too. Despite this claim, the specific proposals set out in the "*Data: A new direction"* do not come anywhere near this ideal scenario. Instead, the protection of the rights of citizens is consistently sacrificed on the altar of 'innovation', in deeply troubling ways. We will set out our concerns in more detail below. Briefly summarized, we do not believe that an adequate and proportionate balance has been achieved between the government's desire to boost innovation and the ever-increasing need to ensure that citizens can be appropriately assured of their

[1] https://www.gov.uk/government/consultations/data-a-new-direction

protection against data harms, and further, that they will have the capacity to take further action to ensure such protection where required.

We have written this response with the above in mind and seek to express precisely where, why, and how the delicate balance between innovation and protection against data harms achieved in the existing data protection regime would be negatively affected by the implementation of the proposed reforms. We believe that for all possible critiques of the existing regime, the appropriate response is not to *lower* protection, but to ensure clarity and legal certainty regarding existing provisions, in order to strengthen protection for data subject. This is *not* achieved in the proposed reforms, in which necessary aspects of data *protection* are in effect framed as burdens, rather than enhancements of, democratic society. Instead, data protection is sacrificed for the sake of innovation. We therefore reject the claim that the proposed new regime successfully manages to *"maintain high data protection standards without creating unnecessary barriers to responsible data use"*.[2]

Our response proceeds by first setting out a general overview of our main concerns, which we have organized into two categories: **(1) discursive concerns** relating to the overall framing of the proposed reforms and the inferences we can draw from this regarding consequences for future data protection law and policy in the United Kingdom; and **(2) substantive concerns** relating to specific reform proposals.

2. Framing innovation as an unmitigated good while ignoring threats to human rights

I. Narrative shifts: Elevating the good of unfettered innovation while omitting fundamental rights

The UK government describes the proposed data protection reform as a *"New Direction."* This begs the question: what was the old direction, and why does the UK choose to deviate from it?

The introductory section to the consultation document does not systematically set out the government's reasons for wanting to deviate from EU data protection law, yet it provides clues: it mentions that *"some existing rules and guidance are either too vague or overly prescriptive,"* and that the new direction will *"deliver better outcomes for people."* These outcomes are described primarily in economic terms, including the "*unlocking*" of "*new economic opportunities*," supporting "*vibrant competition*," establishing a "*pro-growth*" regime, and "*easing the cost of compliance for businesses.*" The "*economic opportunities*" celebrated in the document rely on the understanding that data is "*one of the most important resources in the world*," whose power can be unleashed through innovation. This framing of the justification for a "*New Direction*" is then backed up by the claim that the new direction will bring *"a net direct monetised benefit of £1.04 billion over 10 years,"* and other benefits like more effective data sharing for the protection of national security.

When we look at the framing of the 'old,' European justification for data protection law, the contours of the new direction become even clearer. The 'old' EU GDPR is widely understood to have two main

[2] Page 7 of the proposal "*Data: a new direction*".

purposes: 1) *the facilitation of the free flow of data*, based on the recognition that data processing can bring social and economic benefits, and 2) *the protection and promotion of fundamental rights*, recognising that data processing is only beneficial if it is legitimate, i.e. subject to appropriate safeguards preventing harms and wrongs to data subjects. While the *"New Direction"* exalts the virtues of the first purpose, it fails to recognise the crucial importance of the second.

The consultation document states that the *"New Direction"* is built on the UK GDPR, mentioning data rights for citizens as one of the GDPR's key elements. However, the justification for the proposed data protection reform does not lie in the strengthening of those data rights, and indeed does not refer to fundamental rights at all. The focus of the consultation document is creating *"better outcomes for people,"* without specifying the value that informs the adjective *"better."* The framing of the document, and the proposals derived from it, fail entirely to acknowledge or recognise that the value of data protection lies in its status of a fundamental right, derived from the right to a private life. The consultation document shows no awareness or recognition that the origins of modern data protection law lie in recognising that the systematic storage and access to personal data impacts citizens' fundamental right to private life; and that such storage was a critical enabler of the Holocaust, through which millions of innocent Jews and other 'undesirables' were identified, rounded-up and incinerated with brutal and terrifying efficiency. Even though the condition of having one's rights protected and promoted might be hard to capture as an *"outcome,"* and even harder to capture in pounds sterling, it should be at the core of any legislative reform in a society that wishes to call itself a democracy.

The *"New Direction"* presented in the consultation document avoids fundamental rights language. Instead it couches its discussions in terms of barriers to trade and innovation. This rhetoric fails to capture the *raison d'être* of data protection law, namely the fact that unfettered use of data is not in itself a social good – data processing can only be a good thing if done lawfully within a data protection framework which sufficiently protects fundamental rights and the interests of data subjects. The consultation document emphasises the need for *"responsible innovation."* We posit that responsible innovation does not primarily require the maximisation of economic growth, but rather is closely tied to *lawfulness*, e.g. the setting of legal standards which appropriately distribute responsibility for harms and wrongs caused by data processing and protect fundamental rights. Truly responsible data practices require careful consideration of lawfulness and of fundamental rights protection, which should have been at the front and centre of this consultation document.

This is not to say that European data protection law cannot be improved upon. There is plenty of scope for criticising certain GDPR provisions as being too vague or barely operationalised. However, such criticism should not be used as a pretext for removing protections without due consideration of their critical role in safeguarding both individual citizens from intrusive and dangerous data-driven technologies and the democratic political culture that makes individual freedom, dignity, and autonomy possible. We welcome efforts from the UK government to address gaps in legal protection created by the GDPR, be they caused by legal uncertainty, complexity, or legal vacuum. We also recognise that economic benefit and innovation can be legitimate policy goals. However, we only welcome an emphasis on economic benefits if these benefits go hand in hand with appropriate respect for fundamental rights and civil liberties. Unfortunately, we are dismayed to find that this foundational recognition is entirely absent from the *"New Direction"* presented in the consultation document.

II. A one-sided, unbalanced assessment

The *"New Direction"* discourse is not only unbalanced, it also is not sufficiently backed up by evidence. First, the claim that uncertainty in data protection law stifles innovation is based on assertions and 'evidence' outlined in the accompanying impact assessment document. Even if one is willing to assume that the quantitative estimates of the benefits of the proposals for business are accurate, it is striking that the impact on data subject rights, and the extent to which the reduction of protection will undermine their trust in the data economy is almost entirely absent. The methodology upon which the impact assessment is based, provides a theory of change which is not only dubious in rigour, but also ignores entirely any attempt to take seriously the impacts on the data subjects and citizens as primary beneficiaries of data protection law. Rather, the analysis is almost entirely one-sided with consideration of the impact on data subjects and citizens confined to less than half a page of text under the heading *"Impacts on privacy and trust."* The authors of the assessment state in paragraph 92 that *"the proposed measures are designed to maintain key safeguards and high standards of data protection, while shifting to more outcomes-based requirements and therefore we do not expect the proposals to lead to worse outcomes for individuals."* This claim is pure assertion, without reference to any evidence at all, and fails to recognise that the protections offered by data protection law are not primarily quantitative, but lie in ensuring that basic rights to privacy and associated freedoms are protected by law. The benefits of existing data protection provisions are not, in other words, economic but moral, political and cultural. This does not mean they are *"worthless"* or indeed *"worth less,"* as the impact assessment and the consultation document appear to assume.

Secondly, the document fails to recognise that lowering data protection standards in the UK may well create serious barriers to innovation. Easy data access and sharing from countries outside the EU flowing into and out of the EU market is crucially dependent on those countries ensuring "*an adequate level of protection"* (article 45 GDPR). If the UK adopts rules that significantly lower data protection safeguards for citizens, the EU is likely to evaluate UK protection levels as inadequate – leading to much more uncertainty and many, many times the current amounts of red tape. This could seriously impede the capacity of UK businesses and organisations to access and exchange personal data flowing into and out of the EU. Although the impact assessment offers cost estimates to British businesses if the adequacy evaluation is withdrawn, it is difficult to give credence to those estimates, given the extensive burdens that would then apply to all British organisations seeking to share data with EU organisations, or collect and process data about EU citizens.

In short, the notion that data protection law stifles responsible innovation is unsubstantiated and contentious at best. The contentious narrative deflects the attention from the real concerns that the UK government should be addressing if they wish to safeguard cross-border data sharing.

III. Legal uncertainty

The consultation document repeatedly mentions that one of its core goals is to remove legal uncertainty caused by the existing data protection framework. Although legal uncertainty is a legitimate concern, the consultation document fails to recognise that uncertainty in the interpretation and application of legal texts can never be completely eliminated. Legal scholars have long recognised trade-offs associated with narrowly defined rules on the one hand, and more broadly defined principles on the other. While detailed, rules-based approaches to legal drafting may help to reduce interpretative uncertainty, they do so at the cost of inflexibility, the unavoidable problems of over-inclusion and under-inclusion of the rules, and the danger that legal rules will rapidly be rendered out of date as technologies, social and economic contexts and practices change. This is especially relevant to data protection, as data-intensive practices are constantly subject to technological change, as is explicitly recognised by the consultation document. Moreover, as more and more domains of human activity involve data processing, data protection law must be general enough to cover all kinds of activities which could possibly involve data processing.

Indeed, the 'G' of "*GDPR"* stands for General for a reason. Contemporary European data protection law was intentionally framed in order to provide a general, principles-based framework that could withstand rapidly changing technological innovation and which would be applicable to all domains of human activity involving the use of personal data. While interpretative uncertainty in the meaning of some data protection provisions undoubtedly exists, it is also inescapable. The genius of the law lies in its capacity to provide for mechanisms to settle disputes about the interpretation and application of legal principles, on a stable, legitimate and public basis, namely through judicial interpretation and case law. Moreover, the GDPR provides for the establishment of a national supervisory authority tasked with the provision of information, clarification, and advice to those subject to the Regulation. Although legal uncertainty is a legitimate concern, its negative impacts should not be exaggerated. In any event, concerns about legal uncertainty must be balanced against the real benefits of general principles.

Furthermore, legal uncertainty *cannot* provide an adequate justification for scrapping legal provisions which protect the fundamental rights of data subjects. The proposed means for addressing interpretative uncertainty suggested entail severely curtailing and reducing legal protections and procedures intended to protect the human rights of affected individuals. Take, for example, the proposed scrapping of the obligations to appoint data protection officers; to carry out impact assessments; and to keep sufficient records of activities. All of these protections clarify more general data protection principles – they are concrete ways in which data controllers can ensure that their data is processed lawfully, fairly, and transparently, thereby reducing potential legal uncertainty surrounding those legal principles. Moreover, they do so to protect data subjects from wrongs and harms. If these protections are considered to be unjustified burdens on those wishing to engage in personal data collection and processing, then a convincing case must be made, supported by evidence, to demonstrate that these burdens outweigh the fundamental rights and interests of data subjects. A mere reference to the lack of absolute legal certainty (which is anyway impossible and undesirable for the abovementioned reasons) is woefully insufficient.

If the main problem is indeed legal uncertainty, scrapping provisions which specify the legal obligations flowing from legal principles is not the solution. Instead, the legal provisions on DPO's and DPIA's could be expanded or more legal guidance could be issued by the ICO or the government.

IV. Questionable use of statistics

A final concern about the consultation document arises from poor practices adopted in the collection and use of survey evidence and its misleading use of statistics. In particular, it references the Centre for Data Ethics and Innovation's (CDEI) survey of public attitudes towards data sharing. Not only does this survey repeatedly phrase questions in a one-sided and value-laden manner ("*How comfortable are you with data sharing by researchers to improve knowledge and to help keep the public safe?"*), but the conclusions that the UK Government draws from the data are baffling - if not manipulative.

For example, when respondents are asked what effect data sharing is currently having on the UK economy and society, these were the responses:

AAH1b Thinking now about how data being shared in this way is currently being used. What impact do you think it is CURRENTLY having on the UK economy and society as a whole?	
It is making the situation a lot better	*6*
It is making the situation a little better	*30*
It is making no change to the situation	*34*
It is making the situation a little worse	*6*
It is making the situation a lot worse	*3*
Don't know	*21*
Making the situation better (All)	*36*
Making the situation worse (All)	*9*
NET	*+27*

The UK Government draws the conclusion from this data that there is a *"NET +27%"* on the bottom line. The numbers do not merit these conclusions, and they could instead be interpreted as:
- *"only 36% thinks data sharing improves the UK economy and society as a whole"*
or
- *"64% thinks that data sharing does not impact, or worsens, the situation."*

Similar questionable practices can be seen throughout the survey. Question AAH2_1 of the survey, for example, presents a "*+22 NET"* score of citizens being comfortable with data being shared between the UK government and industry, whereas the data could instead say that:
- "*only 43% is comfortable with such data being shared";*
- *"only 57% is neutral or uncomfortable";*
- *"the majority of the British public does not feel comfortable with data being shared in this way."*

These are just two examples of dozens of contentious cases from the survey. If any of our undergraduate students handled data in this manner for the purposes of university research, they would fail our classes. This falls well below the level that can be expected of both civil servants and legislators, and should not to be used as a foundation for legislative decision-making affecting millions.

3. Objections to specific proposals

Having argued that the general framing of this consultation relies too heavily on promises of economic growth and pays too little attention to lawfulness, to fundamental rights, and to the notion of evidence based legislation, we now turn to the specific reforms proposed within the consultation document. These comments are not ordered in terms of importance. Rather, these concerns must be understood and acted upon together and taken as one whole, in order to ensure that the fundamental rights and interests of data subjects are adequately protected from under any future data protection law and policy framework in the United Kingdom. In this section, we set out a summary of each concern, which is then further explained in Section 4, where we respond directly to the consultation questions.

I. The proposed scrapping of art. 22 GDPR

Article 22 GDPR concerns the right not to be subject to automated decision-making. This was one of the most contentious provisions in the GDPR, and was subjected to extensive debates in its legislative history. The right is indeed highly contextual in its current articulation, and includes numerous conditions and exceptions. Within just a few years of GDPR enforcement, we have witnessed inconsistent and sometimes flawed enforcement of this provision. Hence, there are legitimate possibilities for improving on its scope and application. Even advocates for stronger data privacy protection are critical of the way in which Art 22 GDPR is articulated, albeit often for reasons other than those highlighted by the DCMS. Accordingly, attempts to either streamline and operationalise this right would have the potential to improve the current provision, which could certainly be welcomed by the data protection community.

However, the justification for reforming or even scrapping Art 22 shown in the DCMS report is deeply flawed. It offers no substantive or convincing reasons for the removal of this right, except that the right is difficult to exercise by the data subject and difficult to respond to by the controller. The substance of the right not to be subject to automated decision-making is rooted in the fundamental rights to due process and fair procedure, which have long been regarded as essential requirements of the rule of law, and as central tenets of British administrative law. This response is not the place to discuss at length how Article 22 should be revised. Yet, it is clear that if a right is grounded in the central legal principles of due process and fair procedure, any effort to reform it must be geared towards strengthening it, rather than eradicating it.

II. The proposed scrapping of DPOs, DPIAs, and record-keeping requirements

Data Protection Officers

The requirement to designate a Data Protection Officer (DPO) should not be scrapped in a blanket manner. We acknowledge that the designation of a DPO entails costs for every organisation, and hence is considered particularly unwelcome for small businesses. There are, however, contexts in which having a dedicated individual is highly beneficial to ensure **(a)** clarity and an expert opinion on the application of the law in the context of an organization, **(b)** accountability for compliance with legal standards, and therefore **(c)** for the prevention of harm in high-risk contexts (including law enforcement and other public sector bodies with coercive powers, such as immigration authorities). Further, businesses without sufficient resources for an in-house DPO should be able to avail of an alternative option, such as the use of an external provider. Many organizations already use this much cheaper option of an external DPO service provider for a certain amount of hours per week. Option v(ii) on p.67 should be retained at the very least, but the criteria for assessment should also include the effects and consequences of any decisions made using the processing of personal data.

Data Protection Impact Assessments

The legal obligation to perform and publish data protection impact assessments (DPIA) should also not be removed in a blanket manner. Under current data protection law, a DPIA is only required when processing data which poses a high risk of harming the rights and freedoms of citizens. In those scenarios, the time it takes to perform this procedural check is a small sacrifice in light of the possible harms of the projected processing operations. Removing this safeguard in a blanket fashion places data subjects even further on the back foot against possible data harms, in exchange for limited efficiency gains for data controllers. Considering that the obligation to perform a DPIA already only exists in potentially high-risk situations, requiring such an impact assessment is not unduly burdensome for businesses and cannot be removed without substantive justification taking into consideration the rights and interests of data subjects.

Record Keeping Requirements

Similarly, the legal obligation to maintain records of personal data processing should not be removed, particularly in high-risk contexts. To do so would risk significant data harms to relevant individuals. For example, in the context of an automated decision that may have significant adverse effects on an individual, it would be very difficult for a public authority to offer reasons for said decision – and therefore meet their legal obligations under administrative law – if adequate records of the entire decision-making process are not maintained. Removing current data protection law demands on record keeping will make the application and safeguarding of many other fields of law, as well as

achieving meaningful accountability, much more difficult and therefore deserves a proper evidence based substantiation.

III. The proposed relaxing of the principle of purpose limitation, further processing & the definition of scientific research

The principle of purpose limitation & further processing

The government's proposal (point 54 and beyond) is to significantly diminish the force of the purpose limitation principle. The principle of purpose limitation dictates that a data controller cannot use personal data in whatever way it likes, but is instead largely bound by the purposes for which it originally acquired the data. Purpose limitation is one of the most important principles of data protection law. It is this principle that lays down the rules about what entity gets to use what data, and what the limits are to sharing it with other organizations. As such, it functions as one the absolute pillars of the fundamental rights to privacy and data protection, and of citizens' legal protections against harms caused by unfettered access to personal data, illegal profiling, and biased algorithmic decision-making. The changes proposed by the UK risk undermining these fundamental rights and erode much needed and hard-fought legal protection.

The UK government proposes *"to clarify that further processing for an incompatible purpose may be permitted when it safeguards an important public interest"*, and wishes to *"confirm that further processing may be permitted, whether it is compatible or incompatible, when it is based on a law that safeguards an important public interest."*

Permitting 'further processing' means removing the barrier that is the purpose limitation principle – the cornerstone of privacy and data protection law. The notion that this should be permitted when it safeguards an important public interest is a false dichotomy: the legal protection offered by the purpose limitation *itself is an important public interest*. The notion that diminishing citizens' legal rights in favour of ("*other*"?) public interests, and the idea that an important public interest should categorically override a citizen's right to privacy and to data protection is a blatant attack on the core of the fundamental right to data protection. The strength of human rights is that they cannot be easily overridden – *especially* not by governments. The propositions quoted above undermine this concept of human rights at a fundamental level.

Scientific research

The UK Government's proposal also mentions widening the principle of purpose limitation when processing personal data for research purposes, and changing the definition of research. The GDPR already offers a lot of exceptions to this particular purpose, because scientific research serves a public interest. The UK government would like to take these exceptions a step further, and proposes to change the statutory definition of scientific research to one that explicitly includes privately funded research, performed for private commercial purposes – thereby bestowing upon a part of recital 157 of the GDPR actual legal force.

The problem here, is that this would extend the privileged legal position that is offered to those working for the public good, to people chasing purely private gain, too. This widening of existing exemptions in this fashion is problematic, as it creates a loophole for corporations that are looking for ways to process personal data for any commercial purpose. Consider the exemption for handling special categories of personal data, such as health data: changing the definition of research in the

way the Government proposes, would make it much easier for companies like Amazon and Meta to harvest and analyse medical data of citizens. For they, too, would be allowed to 'research' this data, even when the goal of this research is solely their own financial gain. In practice, changing the statutory definition of research would create an enormous backdoor through which harmful data practices can be whitewashed under the moniker of private research.

Blanketly declaring that any university research is, by definition, carried out in the public interest is similarly problematic. Universities are large, complex organisations which may perform both public and private functions. Declaring that any research performed at a university can base itself on the legal ground of public interest runs contrary to the nature of the research industry, whether at universities or elsewhere. There are thousands of privately funded research projects being undertaken at universities; some serve the public good – many serve purely commercial purposes that do not necessarily equate to the public good. When research is undertaken for commercial motives, the processing of personal data should not be based on the legal ground that the processing is necessary to perform a task carried out in the public interest. The current model of legal grounds ensures that the actual heterogeneity of different research practices is translated into the different legal underpinnings. This ensures that research that clearly is in the public interest can use the eponymous legal ground; research serving purely commercial interests can make use of other legal grounds. The proposal of the UK Government to grant all research undertaken at universities the privilege to base themselves on the legal ground of public interest ignores these important differences. Furthermore, granting university research this statutory status risks derogating from the age-old practice of asking for the consent of research participants. Under data protection law, consent is merely one of six legal grounds – just as legitimate as the ground of public interest. Granting universities the blanket power to use this latter ground seriously risks the position of asking the informed consent of research participants – a cornerstone of ethical research practices.

The consultation document also states that *"[u]ncertainty [about which legal ground to use] may be creating burdens or discouraging useful [scientific] research."* As the use of speculative language suggests, this statement is not grounded in evidence. One of us happens to have been the data protection officer for a research university for some years. Of the hundreds of research cases and consortiums that were guided through the requirements of data protection law, none has ever had to halt their research because of uncertainty over which legal ground should be used. The consultation document ignores the vital role played by research ethics committees, which are mandated under the Declaration of Helsinki to protect the rights of research subjects, by administrative staff, and by data protection officers. Moreover, the GDPR already has very extensive exceptions for scientific research. Given these, research does not typically get barred from taking place based on uncertainty regarding data protection law.

IV. Alignment of commercial, law enforcement and national security processing frameworks

Page 111 of the consultation document discusses the government's ambition to: *"align more closely the commercial, law enforcement and national security processing frameworks, [as] it is important to have the flexibility to bring both further clarity to the police and greater transparency to the public."*

One of the ways in which the government has proposed to do this is:

"To encourage and facilitate the effective sharing of data for law enforcement and national security purposes, we consider there is value in seeking to minimise differences and improve consistency across the commercial, law enforcement and national security processing regimes. Greater consistency between the regimes and additional clarity on data sharing between controllers operating under different rules will ensure that both the public and controllers have a better understanding of how and when data is used to maximise the opportunities to support cross-sector working."

It is unfortunate that these proposals remain vague, with little indication of the substantive changes that may be made. Especially when one considers the magnitude of the processing of data referred to and their potential impact on citizens' lives. As a result, they are incomplete – without specific justifications for specific changes - and it is difficult to assess their suitability and legality of any future action that *might* be taken.

While it may be legitimate and beneficial for the government to improve legal certainty in this area - for example, by exploring whether it is possible to align key terms that are used across the UK GDPR, and Parts 3 and 4 of the Data Protection Act 2018 - the government must ensure to:

(a) acknowledge and reflect in their analysis, that decisions taken in the name of law enforcement and national security are coercive in nature, and subject individuals to limitations of their privacy and individual freedom, their chances and opportunities, and those of their dependants. The processing of personal data in these contexts then is *not* directly equivalent to those decisions taken under the UK GDPR. Because of the potential scope for abuse of state power in these areas, safeguards for fundamental rights are especially important.

(b) take due care to maintain sensitivity towards, and respect for, the different contexts of each decision. The types of decisions that can be made under the umbrella of law enforcement, and those that can be made under the umbrella of national security (including the institutions responsible for their implementation) are *not* directly equivalent, nor are the procedural safeguards afforded to affected individuals under separate legal frameworks. As such, it also follows that the potential harms that can result from their respective processes are not equivalent. Consideration of this must be reflected in any future proposed changes.

V. The proposed changes to the supervisory authority (the ICO)

In light of some of the current UK Government previous interactions with 'reforms' of supervisory authorities, such as the Parliamentary Commissioner for Standards, or the chairpersonship of media regulator Ofcom, any proposed reform to a supervisory authority must be viewed with suspicion. A supervisory authority is independent when it decides for itself what its objectives and priorities are. The UK Government's proposal to submit the ICO to *"strategic objectives and duties that the ICO must fulfil when exercising its functions,"* is an attack on the ICO's independence. The core notion of a liberal democracy abiding by the rule of law, is that the every branch of state authority is subjected to rules and to some form of oversight – including the government. These proposals to bring an independent supervisory authority under the control of the government therefore raise serious concerns about sufficient checks on government power and respect for the rule of law.

4. Conclusion

The UK Government wishes to take UK data protection legislation to a *"new direction"*. Exciting as though it sounds – who doesn't love an adventure? – the legislative proposals formulated are deeply troubling, for many reasons. We could emphasize again the lack of evidence or substantiation backing up the proposals, the lowering of standards of legal protection for citizens, or its believe that it can make legal uncertainty just go away. The manipulative use of survey data and statistics, that falls well below the level that can be expected of both civil servants and legislators. Or the fact that, in a proposal for reforms to law concerned with a fundamental right of citizens – there is not a single bit of serious engagement with the notion of fundamental rights. That the proposal frames fundamental rights as nothing more than burdens to innovate – instead of recognizing their function as one of the core pillars of liberal democracy and thereby their crucial importance for ensuring society prospers. Frankly, there are myriad reasons why the UK Government's *"Data: a new direction"* proposal can be considered, not just a bad idea, but a threat to fundamental rights and the liberal democratic order of the United Kingdom.

If this is the new direction, we hereby call for a change of course.