The Information Commissioner's response to the Ministry of Justice consultation on Human Rights Act Reform

1. Introduction

1.11 The Information Commissioner's Office ('ICO') has responsibility for promoting and enforcing the UK General Data Protection Regulation ('UK GDPR'), the Data Protection Act 2018 ('DPA18'), the Freedom of Information Act 2000 ('FOIA'), the Environmental Information Regulations 2004 ('EIR') and the Privacy and Electronic Communications Regulations 2003 ('PECR'). The ICO is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO provides guidance to individuals and organisations, aimed at helping organisations to comply, and to take appropriate action when needed.

1.12 The ICO welcomes the opportunity to respond to the Ministry of Justice's ('MoJ') consultation on reforming the Human Rights Act 1998 ('HRA'). The ICO is a regulator for information rights legislation. Information rights, and in particular data protection, are underpinned by human rights and should be viewed in this context. Any reassessment of the interpretation of Article 8 and its interaction with Article 10 (freedom of expression) as part of the HRA consultation[1] will directly impact on the work of the ICO and the role it plays protecting the information rights of the UK public, as the regulator.

1.13 The purpose of this response is not to exhaustively address all the issues raised by reform of the Human Rights Act. Rather, it focuses on a number of key issues that both fall within the ICO's remit and have the potential to have an impact on the organisation's work and the outcomes for the UK public.

1.14 At this stage it is difficult to assess the full practical implications of the proposed changes to the human rights regime and therefore the issues raised in this response. The ICO would welcome the opportunity to engage further as the government develops its proposals to better

[1] Human Rights Act Reform: A Modern Bill Of Rights (publishing.service.gov.uk)

understand the potential impact of the proposed changes. This response should be viewed as the beginning of engagement in that regard.

1.2 A trusted data regime

1.21 Much of the ICO's regulatory focus naturally relates to the Article 8 right to private and family life. It is noted however that this is an expansive right that encompasses a good deal more that 'privacy' in the sense it would be understood in relation to data protection. This response is primarily focussed on the intersection of privacy and data rights, rather that issues relating to Article 8 that fall outside the ICO's direct remit (although they are recognised where relevant).

1.22 Equally, data protection is wider than simply being an element of privacy. Privacy does not necessarily engage all examples of information related to individuals in the way that data protection does; and data protection does not have to engage in the 'private' or 'personal' sphere, it also includes the public sphere. This has practical implications, for example in the retrieval of information held by others through Subject Access Requests (SARs).

1.23 The importance of informational privacy in a world where personal data has become increasingly central to the digital economy and the delivery of public services cannot be understated. The ICO supports the government's ambitious National Data Strategy with its first two key missions being "to unlock the value of data held across the economy" and "securing a pro-growth and trusted data regime." The ICO strongly agrees with the government that data-driven innovation and growth relies on people's trust and confidence in how their data is used. The government's response to the consultation on the National Data Strategy notes that, "above all, respondents' feedback confirmed that maintaining a high level of public support for data use will be key to unlocking the power of data. Creating a trustworthy data regime that maintains high data protection standards and enables responsible data use will ensure that the benefits of the data revolution are felt by all people, in all places."[2]

1.24 A trusted data regime relies on having comprehensive and robust data protection law and regulation. Grounding this law in a framework of

[2] Government's Response to the consultation on the National Data Strategy

rights greatly assists in safeguarding this trust. The ICO recognises that the UK fully retained data protection rights when it left the European Union (EU). The UKGDPR now contains these rights in our national legislative framework. With withdrawal from the EU, the European Charter of Fundamental Rights (ECFR) no longer applies to UK law. The ECFR specifically included the general right to the protection of personal data. The effect of the loss of this right has been mitigated by the fact that the right to a private life under Article 8 ECHR still applies. This is a fundamental piece of the wider legislative and constitutional context to support the detail of data protection rights set out in the specific law. The ICO welcomes the government's proposal for the UK to remain party to the ECHR, with the rights, including Article 8, sitting at the heart of a Bill of Rights. However, removing the HRA and implementing some of the government's proposals risks weakening this right as it applies in practice. This in turn could affect individuals' and wider society's trust and confidence in the data regime, ultimately affecting the UK's data driven economy. We ask the government to further look at the proposals in the consultation in light of how they may affect trust in the data regime.

1.25 A trusted data regime, underpinned by the safeguards inherent in data protection and privacy rights, will create conditions for greater engagement with the data reform agenda in the UK. The move toward a data regime that supports growth, innovation and competition will be bolstered by the confidence that comes from public trust. Lessons can be learned from the COVID-19 pandemic that saw engagement with the data driven elements of the response determined by levels of public trust in the programmes that used their personal data.

1.26 Following withdrawal from the European Union, the United Kingdom is no longer party to the EU's Charter on Fundamental Rights and Freedoms. The Charter makes explicit reference to data protection as a element of its Article 8 provision on privacy. We would recommend that the government explores to what extent there is scope in a British Bill of Rights to explicitly refer to data protection under the right to privacy.

2. Legal Context

2.1 The relationship between ECHR and UK data protection law

2.11 The relationship between data protection law and ECHR has a long history. Data protection law, both in the UK and across Europe has largely evolved from Article 8 ECHR. This provides for the right to respect for private and family life, home and correspondence and that "there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

2.12 Concern about the risks to privacy of the individual posed by the growth in the use of computers to process personal information and the possibility that vast quantities of personal data could be transferred across borders and around the world led to the development of two international legal instruments focussed on data protection: the OECD Guidelines in 1980 (updated in 2013) and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in 1981 ("Convention 108").

2.13 These instruments had the effect of applying the right to respect for private life into a more concrete protection for "…personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties".[3] The first UK Data Protection Act 1984 soon followed and has evolved through and alongside European Union law. Throughout this time, ECHR has remained the backbone to UK data protection law. It is referred to in Directive and Regulation Recitals and has been drafted and interpreted in line with ECHR case law.

2.14 The changes to the UK Data Protection Legislation following the UK's departure from the European Union on 31 January 2020 has not changed the relevance of the ECHR to data protection rights. The UK GDPR has been brought into UK law directly from the EU GDPR. In addition, The Agreement on the Withdrawal of the UK from the EU[4] established the terms of the UK's departure from the EU. Its Northern Ireland Protocol includes a commitment to ensure that the UK's withdrawal from the EU

[3] Clause 2 Scope – OECD Guidelines

[4] The EU-UK Withdrawal Agreement | European Commission (europa.eu)

does not result in any diminution of rights, and safeguards or equality of opportunity, as set out in the relevant part of the Belfast (Good Friday) Agreement.

2.15 Although Article 8 ECHR does not refer specifically to the processing of personal data, it does provide that any interference with the right to respect for a private life can only be made in certain circumstances. Different frameworks and rules may apply in the various other scenarios to which Article 8 would be relevant such as in immigration, medical care, or others. The data protection laws set out the relevant approach and framework to considering whether and how personal data can be processed in a way that ensures the individual's rights are safeguarded. UK data protection law is an enabling framework and does not prevent processing taking place as a matter of course, but its proper application ensures that issues such as the sensitivity of the data, the likelihood of harm and the reasons for processing are considered and weighed properly against each other.

2.16 The ICO has largely concentrated on the application of the data protection legislation itself rather than advocating for a more explicit link between the DPA18 and the ECHR (or the HRA). We are confident that that the focus via the data protection framework is sufficient to ensure the wider protections of human rights. It is, however, important that the context and connection between these crucial pieces of legislation is fully assessed in any reforms.

3 HRA Reform and the work of the ICO

3.01 This section of the response seeks to highlight the potential impact of the proposed changes on how rights are balanced, both against other rights and against the public interest. Under the current rights regime there are interdependencies between the HRA and DP law (as set out both above and below) and changes to that regime will inevitably have consequential effects. The subsections below set out the potential affects these proposed changes will have on the ICO's ability to discharge its regulatory duties and its primary objective of upholding information rights in the public interest. It is difficult to accurately foresee the full practical implications of any changes that are currently in the abstract, and

understanding the impacts will require further engagement outside this consultation process.

3.1 The role of the Information Commissioner

3.11 The Information Commissioner is required to act in line with ECHR when carrying out his regulatory duties. These include:

- As a public authority under the HRA, the ICO has a duty to act compatibly with Convention rights

- Under Article 5(1) UK GDPR he is responsible for monitoring the application of the GDPR in order to protect the fundamental rights and freedoms of natural personal in relation to processing and to facilitate the free flow of personal data

- The Commissioner has an established role in assessing the lawfulness of the processing of personal data under Article 6 of the UK GDPR. This includes with respect to the ECHR through the HRA.

The Information Commissioner must therefore act in line with the ECHR when carrying out his regulatory role, in his decision making and in his interpretation of the information rights legislation.

3.12 The Commissioner gives effect to Convention rights through discharging its legal duties which protect those rights implicitly through our regulatory work; and by taking account of Convention rights through its status as a public authority as it discharges those duties. The Commissioner's role is as a regulator for information rights legislation and not human rights more broadly. [5]

3.2 Effects on the work of the ICO from changes to necessity, proportionality and the public interest.

3.21 As a public authority under the HRA, the Commissioner's approach to information rights would be affected by the changes proposed to the

[5] 20161014-ico-response-jchr-inquiry-human-rights-implications-of-brexit.pdf

HRA and thereby the interpretation of the ECHR rights. Given the focus in the consultation on the approach that the courts should have in interpreting human rights in a UK context, it is likely that this will result in different interpretations, particularly on rights related to data protection law, which would then be binding on the Commissioner.

3.22 The ICO has significant concerns about the potential impact of these changes. While we don't prejudge the outcome of what will be an iterative process, there needs to be clarity and detail around the impact of the consultation proposals on the Commissioner's ability to enforce data protection law, in the public interest.

3.23 Under the proposals in the consultation, when determining what is necessary in a democratic society, the court must give 'great weight' to Parliament's view of what is necessary in a democratic society (and the fact that Parliament has enacted the legislation is for these purposes determinative of Parliament's view that the legislation is necessary in a democratic society). Additionally, in determining what is in the public interest, the court must give great weight to the fact that Parliament was acting in the public interest in passing the legislation.

3.24 The new approach to the rights proposed by the consultation is to move away from balancing the qualified rights against each other to place constraints or to weight one interest more heavily than another. This would have a significant impact in relation to the principle of proportionality. The government is proposing that the court must give 'great weight' to Parliament's view of what is necessary in a democratic society. It is important to put the will of Parliament at the centre of the application of the law, and recognise the legitimate weight that should be afforded to that will. But courts already factor in the intentions of the legislature in interpreting the law. Courts also weigh other factors, when appropriate, including the rights of the individuals concerned. The concern for the ICO is the impact of altering the nature of that balance. For example, if the fact that Parliament has enacted a piece of legislation presupposes that this legislation is necessary in a democratic society and in the public interest, what is the impact on courts' or regulators' role in assessing this through the facts of a given case? These proposed changes could have an impact on the work of the ICO and our ability to protect and enforce data rights. It is crucial that the full practical impact of these changes are understood by government before they are made.

3.25 The proposed new approach may also reduce the importance that courts place on the principle of proportionality which plays a key part in ensuring that individual's qualified rights are restricted in as limited a way as possible in a specific situation. In practice, proportionality is vital to assist a public authority in making balanced decisions weighing up the rights of the individual against other rights, obligations or needs of others. This balancing exercise is crucial to the data protection framework for the fair balancing of rights, freedoms, and interests in the context of personal data processing. The nature of this balancing does not rely on clear-cut, categorical answers to conflicts of rights, freedoms, and/or interests, but provides a basic infrastructure for the weighing of the respective considerations.

3.26 The concept of necessity is fundamental across the DPA/ UK GDPR (Article 5 principles, Article 6 lawful bases, Article 9 conditions for processing special category data, Article 23 exemptions, and Schedule 1 DPA18). As the two regimes (HRA and data protection) are inter-twined, there is concern that the changes to the HRA will impact upon the data protection regime. Under the consultation proposals, whenever Parliament enacts legislation relating to the processing of personal data, this fact has to be given 'great weight' by the courts when assessing whether the processing is necessary or in the public interest. The ICO will need to do the same before enforcing the data protection regime.

3.27 The practical repercussions of this could be significant for the application of the data protection regime . Changes in how the concepts of necessity and the public interest are assessed in human rights law will inevitably have an knock on effect on their assessment in data protection law. The likely impact could it more difficult for the ICO to protect individuals data, if public authorities are be able to rely on public interest grounds in a presumptive way. Whilst this will provide more certainty it could create the risk of an unfair starting point that does not allow circumstances and context to be considered

3.28 For both 'necessity' and 'the public interest', changing the current assessments creates the risk of introducing a loop of logic. By definition the 'great weight' attached to Parliament's intention, infused into any legal duty or permission, will pre-empt any assessment by the regulator and make it very difficult to argue that a measure was either not necessary or not in the public interest. The full extent of practical

implications of this change are difficult to assess. However, it could result in a very low bar for any body processing data under legislation regardless of how that processing is undertaken, by arguing that the great weight attached to the necessity or the public interest by Parliament outweighs other considerations.

3.3 ICO application of necessity and balancing the public interest

3.31 As set out above, necessity is a principle of data protection and human rights law; likewise, the consideration of the public interest. The ICO has examples from our work that show both these concepts working in practice and demonstrate how they are applied to data protection decisions without the changes and the potential impacts. These examples show how the ICO, and other public authorities, can sensibly and pragmatically balance necessity against other considerations. Government should consider this when assessing the impacts of the changes outlined above.

3.32 A good example of the application of necessity is the ICO's approach to continuous surveillance in taxis. There may be legitimate reasons, public safety or prevention of crime – for CCTV in licensed cars but the ICO's guidance focusses on encouraging users to assess the necessity of their approach, "…consider the problem you are seeking to address and whether a CCTV system would be a necessary, justified and effective solution. Take into account whether other, potentially less intrusive solutions exist that can achieve the same aim, as well as the effect that each aspect of the CCTV system may have on individuals, and whether their use is a proportionate response to the problem identified."

3.33 On the broader rebalancing of the public interest versus individual rights - the ICO's approach regularly takes into consideration the public interest and recognises when those interests prevail. Included below are a number of illustrative examples:

- Across both our regulatory action policy and or statutory guidance we commit to assessing the public interest as cornerstone of our actions. We assess the public interest in both assessing the behaviour of data controllers and processors, and the public interest in taking regulatory action if data protection has been breached (for

example, to provide an effective deterrent against future breaches or clarify or test an issue in dispute).

- Throughout the COVID-19 pandemic the ICO put the wider public interest in having a fast and effective public health response at the heart of our decisions relating to the use of personal data[6].
- The ICO's code of practice on data sharing utilises assessment of the public interest in a number of circumstances including in relation to special category data, and sharing in an emergency. Controllers will be expected to undertake this assessment and the ICO will take that into consideration in the event of a complaint. The Code and the ICO's work around it, specifically relating to safeguarding children, have emphasised the need to take the wider public interest in protecting children into account when assessing the need for urgent data sharing.

3.4 The balance between Articles 8 and 10 ECHR

3.41 s.12(4) of the HRA already requires courts to give particular regard to Article 10 (right to freedom of expression), when balanced against Article 8 of the ECHR (right to a private and family life). Careful consideration therefore needs to be given to the proposal in the consultation to further strengthen Article 10 by introducing a presumption in favour of upholding the right to freedom of expression (to be clearly spelt out by Parliament).

3.42 Article 8 and 10 rights are both qualified rights and there is currently no further weighting on the face of the law. In addition, in ECtHR case law, the two rights merit equal respect.[7] A person's right to privacy often has to be weighed against another person's right to freely express information. Article 8(2) provides that the protection of the rights and freedoms of others is justification for interfering with privacy. Conversely, Article 10(2) provides that the protection of the reputation or rights of others is justification for interfering with the freedom of expression[8].

[6] https://ico.org.uk/media/about-the-ico/policies-and-procedures/2617613/ico-regulatory-approach-during-coronavirus.pdf

[7] Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [GC], 2017, § 163; Alpha Doryforiki Tileorasi Anonymi Etairia v. Greece, 2018, § 46

[8] Frits Hondius in 1983 A Decade of International Data Protection | Netherlands International Law Review | Cambridge Core

3.43 Given the qualified nature of the rights, setting out in legislation that more weight should be given to one right over another could inadvertently cause harm. Cases involving both Article 8 and 10 are often unique in their nature and have wide and deep implications for both individuals and wider society. Tipping the balance too far in the favour of freedom of expression could reduce protection given by public authorities, including the ICO, to privacy rights. This has implications for data protection for the reasons set out above. The ICO agrees that is right for Parliament to determine the parameters of human rights law in a democratic society but given the impact this is likely to have on how the principle of proportionality applies to competing qualified rights such as Article 8 and 10, it is important that further consideration is given to how an assessment of the facts should be applied in each case as the proposals are developed. The ICO therefore welcomes the proposal to develop more general guidance as part of the framework for a Bill of Rights on how to balance the right to freedom of expression with competing rights (such as privacy) or wider public interest considerations. This will be an opportunity to ensure the principles of necessity and proportionality continue to be applied in the context of the facts of each case.

3.44 The ICO notes the case of *ML v Slovakia*[9] being used in the consultation to demonstrate that in the past the ECtHR has given priority to personal privacy over the right of freedom of expression. It is important to highlight that the facts of this case were particular and its findings should be viewed as such. The consultation does not refer to the significant and sizeable ECtHR case law which has strengthened and protected individual human rights whilst carefully balancing the public interest, or Article 10 considerations[10].

3.45 Within the framework of a new Bill of Rights the ICO supports the consultation proposal to provide more general guidance on how to balance the right to freedom of expression with competing rights (such as privacy) or wider public interest considerations. However, deciding what is in the public interest usually involves objectively considering all the circumstances, factors for and against disclosure and how the public interest is best served, rather than starting from a position that one right

[9] [2021] ECHR 821

[10] https://www.echr.coe.int/librarydocs/dg2/hrfiles/dg2-en-hrfiles-18(2007).pdf

is automatically more important that the other. This more nuanced approach helps to ensure that the public interest is served whilst also mitigating against individual or societal harm in a way that cannot be effectively achieved by elevating the status of the right to freedom of expression above other rights as an in-built presumption.

3.46 The right to private and family life is a condition precedent to the enjoyment of other rights including freedom of expression, freedom of assembly and freedom of religion. In addition to fully extrapolating the direct impacts on privacy (related to data protection) set out above, the government should carefully consider how the impacts on privacy and data protection will have causal effects on other fundamental rights.

3.5 Journalism and Data Protection

3.51 The DPA18 already contains a significant number of safeguards for freedom of expression, through the journalism or 'special purposes' exemption. This means that when an individual or organisation is processing data for the purposes of journalism, they are exempt from many of the obligations in data protection law – for example when there is a reasonable belief that publication of personal information is in the public interest; or a reasonable belief that complying with data protection law would be incompatible with journalism. The ICO's guidance is clear that journalism plays a vital role in promoting freedom of expression in the public interest in a democratic society.

3.52 The ICO is currently in the process of developing a Journalism Statutory Code of Practice under S124 of the DPA18 which looks at how the exemption should be applied in practice and in particular the considerations that are necessary around the balance between protecting privacy and data protection rights and freedom of expression in the public interest. This builds on the guidance the ICO has already published[11]. This has involved extensive consultation with industry, including with the Secretary of State who is required to lay it before Parliament for scrutiny and approval. The statutory status of the Code means that the courts have to take it into account when deciding on cases before them – thereby reflecting the view of Parliament.

[11] https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf

3.53 The code is supported by an impact assessment which acknowledges that although most journalism on a day-to-day basis does not cause any data protection concerns, when this does occur, the power and influence of the press and others, especially in the digital world, means that processing personal data for journalism has the ability to cause substantial harm to individuals. This includes physical harm, material harm (such as financial harm) and non-material harm (such as emotional distress). The assessment also acknowledges that a wider societal harm may occur if effective public interest journalism is undermined by a lack of public trust. As journalism has a special role to play in the free flow of communications and holding the powerful to account, inaccurate news for example, may be particularly damaging in this regard. In view of the above, this code has an important role to play in helping those using personal data for journalism to balance freedom of expression and data protection in the public interest.

3.54 The code will include guidance on how to apply the special purposes exemption[12]. One key factor is deciding what is in the public interest. This includes considering the circumstances, balancing relevant factors for and against publication; and judging how the public interest is best served by publication. The code explains the broad operation of the public interest test involving general public interests and specific public interests, and what factors it may be relevant to consider. It also recognises the wider public interest in in journalism and freedom of expression. These tests are based on well-established general principles developed by the UK judiciary in domestic case law about how to perform this balancing test and reconcile, proportionately, competing rights and interests. This draws on the judiciary's experience in complex adjudication of competing rights and interests.

3.55 We would be very happy to discuss this further with the Ministry of Justice to see how the Code can assist with ensuring concerns about the balance between privacy and journalism in the public interest are addressed.

[12] Those processing personal data for journalism do not have to comply with many of the usual requirements of data protection law when personal data is:
being used for journalism;
with a view to publication;
there is a reasonable belief that publication would be in the public interest; and
a reasonable belief that complying with data protection law would be incompatible with journalism.

3.6 Article 8 claims on public authorities

3.61 The consultation raises issues around the burdens placed on public bodies (e.g. the police) by Article 8 claims. We acknowledge the pressures facing public bodies, but despite this pressure we reiterate that decisions around collecting, retaining or disclosing personal data need to be taken in line with data protection law. The disclosure of personal data is an interference to respect for private life, and requires justification[13].

3.62 There is considerable Article 8 case law involving the police in particular, retaining data (DNA profiles, fingerprints and cellular samples) indefinitely and indiscriminately with a limited ability to obtain destruction was held to be in breach of Article 8[14]. A police policy of retaining photos of individuals arrested but without charge constituted an interference with Article 8[15]. However, there is also caselaw that sets out where public authorities, notably the police, can retain data in line with Article 8 rights.

3.63 Both Article 8 and data protection legislation act to protect individuals against overreach or malfeasance by public authorities. They oblige those bodies to both consider the necessity of their actions and justify any interference with rights. The ICO has demonstrated (including the examples above) how a considered approach from public authorities, regulators and courts in the application of rights can result in pragmatic outcomes.

3.64 The ICO has a series of examples from our operational experience that demonstrate the importance of maintaining trust in public authorities through accountability, including a data protection regime underpinned by Article 8 privacy rights. These include:

- The impact on victims of serious sexual offences of unnecessarily intrusive searches of their past history and their loss of confidence in the criminal justice system.
- The failure to ensure the police gangs intelligence database was accurate leading potentially to children and victims of crime being denied education and housing opportunities.

[13] Hilton v UK (Application no 12015/86) 57 DR 108
[14] S and Marper v UK [2008] ECHR 1581
[15] RMC and another v Commissioner of Police of the Metropolis [2012] EWHC 1681 (Admin)

- The failure to assure patients of the security and privacy by design elements of the GPDPR proposals leading to loss of confidence and participation by the public and the scheme being delayed.

The ICO would be happy to further engage with the Ministry of Justice on our experience in this regard.

4 Other Issues of Concern

4.1 Permission stages

4.11 The consultation suggests that people lose trust in a system when frivolous and spurious cases come before the courts and that this devalues the concept of human rights. It states that it is wrong that the burden is on public bodies to apply to courts to strike out spurious claims. The government proposes claimants have the responsibility to show that their claim has merit by passing an initial permission stage which must show that they have suffered a 'significant disadvantage'. This could include a second 'overriding public importance' limb, available in exceptional circumstances if the first limb is unsuccessful.

4.12 The ICO would urge the government to provide clarity on how the current 'victim test' (s.7 HRA) differs from the 'significant disadvantage' test. If the threshold is raised, there is a risk that genuine claims (where the extent of harm does not come to light at the permission stage) might not be able to proceed.

4.13 It is also worth highlighting that if claimants are not able to apply to courts for breaches of their right to a private life under ECHR Article 8 then where breaches (or potential breaches) involve the unlawful processing of personal data there is a likelihood that there will be an increase in complaints to the ICO and applications to the courts under UK GDPR. While it might be argued that is this a more appropriate and more proportionate route for these claims, that impact should be properly assessed.

4.2 Adequacy

4.21 The government will be aware that the European Commission considered that the UK's domestic and international commitments to human rights were particularly important elements for its adequacy decisions in respect of the UK. The Human Rights Act 1998 and the European Convention on Human Rights (ECHR) are referenced extensively throughout both decisions. For example, recital 120 of the adequacy decision under the EU GDPR[16] and recital 161 of the adequacy decision under the EU Law Enforcement Directive[17] stress the importance of the UK adhering to its international obligations under the ECHR. Cooperation on law enforcement and criminal justice between the UK and the EU under the Trade and Cooperation Agreement is also underpinned by the UK's human rights commitments.[18]

4.22 It should be further noted that a number of international commitments including Convention 108 (and its future revision as Convention 108+) are to be interpreted in line with the jurisprudence of the ECtHR. As the Convention for example is specifically referred to in the Adequacy Decision for the UK, the Government should be aware that failure to adhere to the UK's commitments under the ECHR may affect compliance with those instruments and represent a risk to adequacy.

4.23 In order to maintain EU adequacy decisions, the Government should ensure its proposals continue to effectively implement the ECHR in British law. A November 2020 report estimated the impact on the British economy of not having such decisions in place as a cost of £1-1.6 billion.[19]

4.3 Questions around the definition of "public authority"

4.31 The consultation (Para 266-269) raises issues around the definition of public authority and the discharge of public functions by private bodies. Changing the definition of a public authority and limiting their duties under the Human Rights Act could have the effect of enabling public authorities to argue that they were unable to respect, protect or fulfil an

[16] adequacy decision under the EU GDPR
[17] adequacy decision under the EU Law Enforcement Directive
[18] Article 524, Trade and Cooperation Agreement
[19] *'The Cost of Data Inadequacy'*, New Economics Foundation and UCL European Institute, 2020

individual's human rights where they are carrying out duties under laws made by Parliament. We need to more fully understand the implications of this, for example, on whether it would effect the ability of the Information Commissioner to take action against some bodies currently considered public authorities, in the future.

4.32 The government highlights the difficulties around defining a 'public authority'. A comparison can be made here with the definition of a public authority under the FOI and EIR regimes and what is appropriate in an era when public services are increasingly delivered by a range of bodies in the private, charitable and public sectors. The ICO has argued that that the FOI and EIR regimes should be extended to any organisation when it is delivering public services funded by public money, to increase transparency and accountability in decision making. We therefore do not think it would be helpful if the intention of this proposal is to narrow the scope of the definition of a 'public authority'. This is not the direction of travel in other constituent parts of the UK, such as Scotland, and creating inconsistencies in a UK wide piece of legislation could cause confusion in implementation and enforcement. We would be happy to discuss further with government on this issue.

4.4 Introducing the idea of responsibilities into the human rights framework

4.41 Potentially, this would mean that an individual's behaviour could be considered when deciding whether it was acceptable to limit their human rights and in deciding what damages to award to the person. This includes not just a person's conduct during the case in question but for their whole lives. It needs to be clarified if this would mean that not everyone would be entitled to the same rights and would move the UK away from universality as a principle of human rights.

4.42 The government aims "to build an element of responsibility explicitly into the Bill of Rights by permitting UK courts to consider the claimant's conduct in deciding whether or not to award a remedy. The court will be invited to hear about the lawfulness of the claimant's conduct in the circumstances surrounding the claim but also be empowered to consider relevant past conduct, such as whether the claimant has respected the rights of others". This two forms of concerns from an ICO perspective. The first is around the universal application of human rights

– there need to be clarity in how to reconcile this with the changes proposed. And what the impact will be on bodies who enforce rights. Secondly, there are direct data protection implications for examining "past conduct" including how authorities will apply purpose limitation and data minimisation if intending to collect data about a claimant's past.

5 Conclusion

5.11 The importance of data to growth, innovation and competition is recognised across government and all sectors of the economy. The success of this will be predicated on a trusted data regime that us currently underpinned by data protection law and human rights protections. Changes to how these protections operate raise a series of risks and concerns about the impact on the ability of the ICO to protect individual's data and privacy rights.

5.12 This response also sets out a number of practical examples of how the ICO deals with the concepts such as necessity and the public interest, which are the subject of potential change, in a considered and pragmatic fashion. These should be instructive to government in deciding the need for those changes.

5.13 Finally, it is difficult to judge the full impact of potential changes and therefore charting the risks comprehensively. Nor can this response deal exhaustively with all the issues raised in the consultation. The ICO will want to engage fully in discussions round changes to the law that directly impact upon its remit. The content of this response is the starting point for further engagement with Ministry of Justice on the risks and concerns raised here.

8th March 2022