Information Commissioner's Response to the Data Protection and Digital Information (No 2) Bill (DPDI No 2 Bill)

About the ICO

The Information Commissioner has responsibility for promoting and enforcing the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA), the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations 2004 (EIR) and the Privacy and Electronic Communications Regulations 2003 (PECR). He is independent from the Government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken.

Introduction

The Data Protection and Digital Information (No 2) bill (the DPDI bill) was introduced to Parliament on 8 March. It is an important milestone in the evolution of the UK's data protection regime.

Responsibility for developing policy and for making changes to the legislative framework sits with Government and Parliament. The ICO is independent from the Government and our role is to carry out the duties set out in the current, and any future, legislative framework. I welcome the DPDI bill as a positive package of reforms that allow us to continue to operate as a trusted, fair and independent regulator. The bill protects people's rights and freedoms, whilst also providing greater regulatory certainty for organisations and promoting growth and innovation in the UK economy.

The bill is the result of wide public consultation. This includes robust and constructive engagement between my office and the Government throughout the development of the data protection reforms[1]. In line with the requirements of Article 36(4) of the UK General Data Protection Regulations (UK GDPR)[2], we have provided our expert advice during the

development of the draft legislation. We will continue to provide constructive input and feedback as appropriate during the Parliamentary scrutiny and approval process.

We provided a comprehensive response to the Government's original consultation, 'Data: A New Direction' on 6 October 2021. On taking office in December 2021, I also set out my concerns on a number of the proposed reforms, including the role of the Secretary of State in appointing the CEO and in approving all significant or novel ICO guidance. I felt strongly that as they stood, those reforms would reduce the ICO's independence, and that the proposed changes to our guidance production would also reduce regulatory certainty for organisations. I also felt that to retain our independence from the Government, it was important for the CEO to be appointed by the Chair and Board, not the Secretary of State.

I'm pleased that the Government has taken my concerns on board and made changes that mean the bill now maintains our regulatory independence and promotes trust and confidence in the regulatory process. This means the DPDI bill has moved to a position where I can fully support it.

Providing clarity and regulatory certainty

The changes in the bill reflect the fact that the ways in which personal information is used are evolving, and it is right that the way we regulate evolves to keep up. I welcome the changes that provide more certainty to organisations, empowering them to use personal data responsibly, in ways that will generate social and economic benefits, while still ensuring people are protected. This includes the changes to support organisations to use personal data for research, the importance of which was demonstrated powerfully during the pandemic. The bill also clarifies the definition of what constitutes scientific research and make the rules around further processing of data clearer.

The bill also gives more confidence to organisations to rely on the legitimate interests lawful basis and to further process data. As well as the bill specifying circumstances in which the existing legitimate interests lawful basis for processing can apply, Schedule 1 sets out 'recognised legitimate interests' where no balancing test is required eg in situations such as crime prevention and safeguarding, where nervousness about sharing data can cause real harm. Schedule 2 sets out further processing purposes that organisations can assume are compatible. Organisations

will still need to consider necessity and proportionality but, in taking this approach Government has taken on the responsibility for assessing where the balance lies between legitimate interests and people's rights and freedoms, and whether further processing is compatible, at a generic level.

The bill also clarifies the rules around international transfers. While the approach and standards remain consistent, the clarifications are intended to help organisations feel more confident about taking a risk-based approach when using existing mechanisms.

There is more clarity for organisations about how they respond to subject access requests (SARs). SARs are a key data protection right, but people can sometimes misuse them in ways that create unnecessary burdens for organisations. The change allows organisations to refuse requests that are vexatious or excessive, rather than the current language of manifestly unfounded. This is based on feedback from organisations that this is easier for them to understand. The revised wording should be clearer for organisations, while still protecting rights.

Whilst the bill increases certainty overall, there are some areas where it could be clearer. These are set out in Annex 1.

Ensuring a proportionate approach to demonstrating accountability

I welcome the introduction of a more flexible and proportionate approach to demonstrating accountability. While organisations must remain accountable for how they use our personal information, it is right that we empower them to demonstrate accountability in ways that work for them, rather than requiring a one-size-fits-all approach. The risk-based approach that the Government is implementing should achieve this, where prescriptive requirements are focused on organisations carrying out high risk processing. However, for greater clarity and certainty, we would welcome more detail in the legislation on what constitutes high risk processing.

Organisations will also need to be more accountable to people, as a result of new requirements for them to put in place a formal complaints procedure.

Protecting people's rights and freedoms

The key objective of any data protection framework is to provide appropriate protections for people's rights and freedoms. The Government has made a number of important decisions that will maintain our high standards of protection in the UK. We raised concerns about the initial proposal to remove the right to a human review of AI processing decisions that affect people, and are pleased this has been retained. We welcome the fact that the right of access to personal data remains free of charge in most circumstances. Also, that the Government has not taken forward the initial proposal to introduce a cost ceiling for subject access requests, that we did not support. We also welcome the changes that will make it clearer that organisations can only further process data originally collected on the basis of consent in specified circumstances, and that require organisations to have a clear complaints process.

It is also clear that there are a number of other key reforms which will have a positive impact on maintaining our high standards of protection, including the additional enforcement powers for the ICO. We've highlighted these further below.

Reducing burdens on organisations, and promoting growth and innovation

Alongside strong protections, we need to make sure that our data protection framework is as easy to navigate and use for organisations as possible. Responsible use of personal data that people can trust has significant potential to contribute to the UK's economic prosperity. There are a number of changes in the bill that will meet these objectives and I am pleased to see them included. These include:

- making the research, archive and statistics purposes (RAS purposes) provisions easier to navigate and understand;
- simplifying the requirements when organisations rely on these provisions when carrying out processing for these purposes;
- making the automated decision-making provisions simpler to apply; and
- making it easier for organisations to use the legitimate interests' lawful basis for a number of specified purposes.

As noted above, the accountability requirements have been streamlined to focus on high risk processing. This will free up many organisations from

keeping mandatory paperwork and instead give them more flexibility to implement their own approach. Non-commercial organisations, such as charities, NGOs and political parties, will be able to contact people who have expressed an interest in their cause without consent. This is because the direct marketing rules will change to put them on a par with commercial organisations.

The rules around electronic communications and 'cookies' are being clarified so that organisations will be able to deploy essential software security updates more easily. The Government has also introduced a power for the Secretary of State to make regulations that would introduce an 'opt out' model for cookie consent to improve people's experience of the internet.

Supporting the delivery of public services and the protection of public security

We know that the use of personal data is vital for public service delivery and the protection of public security. To support these objectives, the Government has made some key changes, including:

- shifting the responsibility for deciding whether data can be used for public tasks from private firms to the public bodies they work with;
- allowing joint controllership arrangements between law enforcement bodies and the intelligence services when required to protect national security; and
- extending disclosure powers under Section 35 of the Digital Economy Act 2017 (DEA 17), so that data can be shared to improve delivery of public services to business undertakings.

Supporting regulatory effectiveness

It is vitally important to maintain a strong and effective regulator and we are pleased that the Government has made a number of changes that will significantly improve the ICO's ability to function effectively. I am particularly pleased to see the strengthening of our enforcement powers. While I prefer to work with organisations where I can, supporting them to build in data protection from the start, the additions to ICO powers will help me to take action to ensure people are protected quickly and effectively, where needed.

Amongst the most significant of these is the increase in fines for breaches of PECR, which will help us tackle predatory marketing calls which often

target those at most risk of harm. There are also other changes to improve our ability to tackle nuisance calls. These include a change to allow us to take enforcement action against organisations on the basis of the number of calls they generate, rather than just the number that are connected. The bill will also introduce a 'duty to report' on communications providers to inform us of suspicious levels of traffic on their networks.

Alongside our expanded enforcement powers, I welcome the changes to the way organisations handle complaints; and our new explicit power to refuse complaints that have not exhausted an organisation's complaints procedure or are vexatious or excessive. These changes should help us free up more resources to focus on tackling the greatest harms to people and issues where we can have the biggest impact.

We will also be required to fulfil new obligations to establish stakeholder panels to inform the content of our codes of practice and to develop and publish impact assessments on our key regulatory products and interventions. This will contribute to our aim to be a transparent regulator and deliver on our obligations to ensure we contribute to the UK's economic prosperity.

Maintaining regulatory independence and accountability

The bill brings some significant changes to our governance arrangements that will maintain our independence and enhance our accountability. Having an independent regulator, that is also properly accountable to Parliament, is vital for a properly functioning data protection regime. It is also key to maintaining the UK's adequacy status from the EU, which we know is a priority for so many of our stakeholders.

Our governance arrangements will be modernised to a board and chief executive model. This will enhance our resilience and diversity at senior decision-making level. His Majesty will appoint the Chair of the board via Letters Patent, the same process used for my appointment. As we proposed, the Chief Executive will be appointed by The Chair and Board, rather than the Secretary of State. This will avoid any perceived conflict of interest that could have occurred.

There are a number of other new requirements that will improve our transparency and accountability as a regulator. This includes the requirement to have regard to, but not be bound by, a Government

statement of strategic priorities that will be approved by Parliament. Another is the clear parliamentary articulation of our regulatory framework via statutory objectives and duties. This includes the principal objective of securing an appropriate level of protection for personal data, having regard to the interests of individuals, organisations and matters of general public interest.

There will also be a limited power for the Secretary of State to approve statutory codes of practice, with new transparency obligations if a decision is made to refuse, and final approval remaining with Parliament.

Conclusion

These changes respond to the particular circumstances and needs of the UK. However our engagement with stakeholders has made it clear that our relationship with the EU remains of central importance, and the certainty a positive adequacy decision from the EU provides is a top priority. I welcome the Government's commitment to the importance of maintaining our adequacy status. Adequacy does not require a carbon copy of the GDPR and these changes maintain the high standards that both the UK and EU are committed to. Whilst ultimately a decision for others, in my view the proposed changes in the bill strike a positive balance and should not present a risk to the UK's adequacy status.

While overall the bill represents a positive and balanced package of reforms, as with any legislation there are some points that would benefit from additional clarity. These technical points, which we have already shared with the Government during our ongoing engagement, are summarised in Annex 1. These reflect our formal response to the Government's consultation of the ICO under Article 36(4) of the UK GDPR.

Annex 1 - Information Commissioner's Response to the Data Protection and Digital Information (No 2) Bill (DPDI No 2 Bill)

This annex complements the Information Commissioner's Response to the Data Protection and Digital Information (No 2) Bill (DPDI No 2 Bill.

Introduction

We welcome the Data Protection and Digital Information (No 2) Bill, which provides a range of benefits for both people and businesses. We have had an open and constructive dialogue with the Government as the data reform proposals have developed into draft legislation. We have drawn on our experience regulating the current legislative framework to provide detailed technical advice. This document summarises where:

- we think drafting could provide further clarity; or
- we do not think drafting reflects the policy intent.

It should be read alongside the accompanying response from the Information Commissioner.

Part 1 Data protection

Definitions

- **Clause 1 – Information relating to an identifiable living individual**

The drafting introduces a new element to the definition of personal data – specifically, the test for when an individual is identifiable by a third party. Currently, the test involves looking at all the means reasonably likely to be used to identify someone, either by the controller or by another person. Information is personal data if a third party could identify the people concerned using reasonable means.

The new drafting means that the controller first judges whether a third party is likely to obtain the information. If the controller does not intend to identify people for its own purposes, and judges that a third party is unlikely to obtain the information, then it's not personal data, irrespective of how easily people could be identified. This means that the controller

has no data protection obligations. Therefore, they do not need to consider things such as whether its anonymisation or security measures are robust enough to minimise privacy risks to people (eg in case of unauthorised access or accidental disclosure).

This amended definition of personal data therefore creates a theoretical privacy risk. It's possible that a third party could gain access to data in some cases, despite a controller's judgement that this was unlikely to happen. If this happens and the third party can in fact identify living individuals, those individuals do not have recourse under data protection law for the failure to protect their data. This is because the information would not fall within the definition of personal data.

Arguably, the drafting also creates a circular situation. If a controller judges the information is difficult to access and so is 'unlikely' to be obtained, then it is not personal data. But if it's not personal data, then it doesn't have to be protected, which in practice increases the risk that it may be obtained. Even if an organisation puts some protections in place to reduce the likelihood of access, those measures do not need to take account of the nature of the information and the potential risks to individuals.

We do not oppose the clause overall, given that many of the other changes in the clause do help to clarify the definition of personal data. Also, we have no existing evidence of particular cases where information was previously in scope and will now fall out of scope. However, the drafting creates a theoretical privacy risk and is potentially confusing.

- **Clause 2 – meaning of research and statistical purposes**

The research, archive and statistics (RAS) provisions allow data to be kept indefinitely, provide exemptions from some data subject rights, and allow an assumption of compatibility for the re-use of data (unless the data was originally collected under consent).

Clause 2 draws on wording from Recital 162 of the UK GDPR. It only allows processing for statistical purposes to benefit from the RAS provisions if:

- the results of the statistical processing are aggregate data that is not personal data; and

- neither the original personal data, nor the results, are used to make decisions about the original data subjects.

Our view is that aggregate data may sometimes also be personal data (if the 'key' that would allow de-aggregation and reidentification of a data subject is retained). This means that this drafting would prevent a data controller from benefitting from the RAS provisions if they have:

- taken steps to aggregate personal data; but
- retained the 'key' that would allow de-aggregation.

We assume this is the Government's intention.

- **Clause 3 – consent to processing for the purposes of scientific research**

This clause incorporates the "broad consent to processing for research purposes" wording from Recital 33 into the legislation.

We have some comments about the clarity and structure of this clause. In particular:

- We suggest that the text inserted would be better placed under Article 7 rather than under Article 4(7), as we consider that it provides detail on the conditions for consent, rather than the definition of consent.
- Regardless of which article the new text is inserted into, we consider that the words "it does not fall within that definition because (and only because)" should come before each of the criteria (a) to (d), rather than as part of (a). So that it applies to each of (a) to (d).
- Regardless of which article the new text is inserted into, we consider that using the word 'purposes' in subsection (b) risks introducing confusion about the level of specificity required for purposes in other parts of the legislation (particularly in relation to privacy information where we would generally consider that 'scientific research' is a specific enough purpose). We therefore suggest that it would be preferable to say "(b) at the time the consent is sought, it is not possible to be specific about the precise research activities for which the personal data will be processed".

Data protection principles

- **Clause 6 – The purpose limitation**

We consider the addition of "or on behalf of the controller" in Article 5(1)(b) is inconsistent with the language used elsewhere in the legislation (where there appears to be no need to specify that provisions apply both when a controller is acting in its own right and when it instructs a processor to act on its behalf). We think this wording is unnecessary and there is a risk that including it here but not elsewhere could be taken to be more significant than it is. It may also be misinterpreted as meaning that processors have a responsibility to assess compatibility (rather than just to act on the instruction of their controller).

We think it is debatable whether the explanatory note on Article 6(1) lawful basis/Article 8A compatibility, as currently drafted, adds to the clarity of the legislation or reintroduces ambiguity. We understand that the intention is to make it clear that if controllers can satisfy an Article 8A provision then it is likely that they will also be able to satisfy a corresponding Article 6(1) lawful basis for processing. However, we think the explanatory note could be read to suggest that controllers do not need to satisfy an Article 6(1) basis for the further processing (nor advise the data subject).

Data subjects' rights

- **Clause 7 – vexatious or excessive requests by data subjects**

This clause changes the current threshold for refusing to act upon a request from a data subject from "manifestly unfounded or excessive" to vexatious or excessive. It adds the new Article 12A (vexatious or excessive requests) into the UK GDPR and section 204A (vexatious or excessive) into the DPA 18.

We consider there to be some inconsistency in the language used in the new Article 12A provision. Article 12A(4) indicates that controllers must have regard to the circumstances of the request, along with regard to the criteria set out in Article 12A(4)(a) – (f). However, Article 12A(5) gives examples of requests that may be vexatious. We think that both 12A(4) and (5) should direct the controller to consider all the circumstances and it should be made clear that both are non-exhaustive lists to help future proof this provision.

- **Clause 9 – information to be provided to data subjects**

Article 14(5) currently allows an exception from providing transparency information where an organisations has not collected personal data directly from the data subject and provision of this information would constitute a disproportionate effort. Clause 9 mirrors this exception within Article 13 where organisations have collected personal data directly from a data subject for research purposes. However, it does not include the following wording from Article 14: "likely to render impossible or seriously impair the achievement of the objectives of the processing for which the personal data are intended".

We think this could be interpreted as meaning that where organisations have collected data directly from the data subject, it is not possible to claim exception from providing transparency information on these grounds (eg where full transparency may undermine research objectives, or the cost of providing privacy information would impair the objectives of the research).

Automated decision-making

- **Clause 11 – automated decision-making**

This clause provides that, in relation to Part 4 processing, if there is no opportunity for human involvement in an automated decision, then that decision will be "a decision based on entirely automated processing". It is, however, silent on what the effect is if there **is** an opportunity for human involvement. Our understanding is that the Government's intention is that a mere 'opportunity' for human involvement in a decision will not be sufficient to take a decision outside of the scope of "a decision based on entirely automated processing". Organisations would have to exercise this opportunity to have this effect. It would be useful to make this intention clear in the drafting or the explanatory notes.

Obligations of controllers and processors

- **Clause 12 – General obligations**

The responsibilities of controllers and processors to secure and protect personal data has changed (eg in Articles 24, 25, and 28). The Government has replaced the drafting of "appropriate technical and organisational measures" with "appropriate measures, including technical and organisational measures". We believe this is intended to allow

controllers greater flexibility but we are unclear about what would constitute "appropriate measures" which would not be considered "technical and organisational measures". We have not been given any examples by the Government. Although unlikely to result in a significant risk to data subjects, it would be helpful to clarify further the policy intent of the change, so we can provide guidance to controllers and processors.

- **Clause 15 – Duty to keep records**

The Government has amended the exemption from record keeping requirements. It now applies to all organisations unless their processing is likely to result in a high risk to individual's rights and freedoms. We will need to provide guidance on what constitutes high risk processing, which we comment on further in relation to clause 17 below.

- **Clause 17 – assessment of high risk processing**

The Government has decided to replace the requirement to produce data protection impact assessments (DPIAs) with risk assessments. Risk assessments are similar to DPIAs but there is less prescription about what they must cover. Risk assessments will only be mandatory when organisations process personal data in a way that is likely to result in a high risk to people's rights and freedoms. The bill removes Article 35(3), which provides additional detail by setting out circumstances in which a DPIA is definitely required. It also removes the Commissioner's current duty in Article 35(4) to create and publish a list of the kind of processing operations that require a DPIA (ie types of processing that are likely to result in a high risk). These aspects of the legislation are replaced with a new duty on the Commissioner at Article 57(1)(k) to produce a document containing examples of the types of processing he considers are likely to result in a high risk to individuals' rights and freedoms for the purposes of the accountability provisions as a whole (ie appointing an SRI, record keeping and risk assessments).

We are comfortable with the new duty on the Commissioner under Article 57(1)(k) to produce a document about high risk processing. We will also develop guidance on the other revised accountability requirements. However, we think that the Government's approach may leave controllers and processors with considerably less certainty about when their processing is high risk and therefore in scope of these provisions, particularly in the event of challenge through the courts.

In our view, the detail in Article 35 (3) was a helpful and clear legislative backstop. We think it would be beneficial to retain it, or provide some detail in the legislation of the types of processing that are likely to be high risk in some other way.

International transfers of personal data

- **Clause 21 – Transfers of personal data to third countries and international organisations.**

We support the overall policy intent behind these proposals to provide clarity to stakeholders on how adequacy decisions will be made. Also, to help data controllers and processors understand their obligations more clearly when putting in place alternative transfer mechanisms. However, we think the changes to Chapter 5 of the UK GDPR may benefit from further clarity in some areas.

For example, referring to both tests for adequacy, in Article 45B, and for appropriate safeguards, in Article 46(6), as the "Data Protection Test" may lead to confusion. Although this can be clarified in our guidance, it would be preferable to make this explicit in the legislation.

There are also areas where the drafting of the provisions seems to introduce a level of ambiguity, although it is seeking to clarify existing practice when the Government assesses the adequacy of third countries . We welcome the legislative language confirming that adequacy regulations approving the transfer of data to a third country or international organisation **'may only be made'** if the Secretary of State considers that the data protection test is met. The clause also specifies that the Secretary of State may have regard to any matter they consider relevant, including the desirability of facilitating transfers of personal data to and from the United Kingdom when deciding to make adequacy regulations.

The Government has been clear on its position that the data protection test must be met for adequacy regulations to be made, and that in their view there is no conflict. However, the interaction between 46(6) and the requirements of Article 45B (2), which sets out the factors that the Secretary of State must consider when determining whether or not the data protection test has been met, would benefit from being clearer. It would be helpful to clarify that the matters the Secretary of State may consider do not outweigh or take precedence over the need to meet the

data protection test. We would welcome explicit clarification in the legislation that there is a distinction between the decision making about which countries to make adequacy regulations for, and the decision about whether the data protection test is met for any such country. This would improve regulatory certainty.

In terms of the scope of adequacy regulations, Article 45B(3)(c) states that they are to apply to transfers "from the UK". This may be restrictive to controllers based outside the UK but caught by the scope of the UK GDPR due to Article 3(2) who would otherwise benefit from the adequacy decision.

Safeguards for processing for research purposes etc

- **Clause 22 – Safeguards for processing for research purposes etc**

We think that this clause contains a contradiction as it provides that personal data (by definition, information from which a living individual can be identified) can only be processed in a manner that does not allow an individual to be identified.

We assume that the Government's intention is to make it clear that the most data protection friendly way to carry out research is to use anonymised rather than personal data and that personal data can only benefit from the research provisions, if that is not possible. However, we don't think the current drafting achieves this.

We also think that the intention could be to make it explicit that personal data may be processed for research purposes if that processing amounts to the anonymisation of personal data, to create a new data set of non-personal data to be used for research purposes. But again, we do not think the current drafting achieves this.

Intelligence services

- **Clause 25 – joint processing by intelligence services and competent authorities**

The proposed new section 82A(2) states that, "the Secretary of State may only designate processing by a qualifying competent authority that is carried out by the authority as a joint controller with at least one intelligence service". As a joint controllership arrangement is only possible

once the designation has been made, we suggest that the drafting needs to reflect this. To the effect that the Secretary of State may only designate processing by a qualifying competent authority that **will be** carried out **following the issue of the designation notice** by the authority as a joint controller with at least one intelligence service.

Information Commissioner's role

- **Clause 32 – Vexatious or excessive complaints made to the Commissioner**

Clause 32(4) of the DPDI omits Article 57(4) of the UK GDPR which permits the Commissioner to refuse or charge a fee for responding to requests that are manifestly unfounded or excessive. Section 135 of the DPA 18 provides a similar basis for the Commissioner to refuse or charge a fee for responding to requests. However, in our view it is narrower in scope than Article 57(4) because it only applies where a request is from a data subject or data protection officer and is deemed manifestly unfounded or excessive. Article 57(4) allows the Commissioner to refuse or charge a fee to act upon manifestly unfounded or excessive requests, regardless of who the request is from. In our view, section 135 should be amended to mirror this approach.

Retaining a more widely scoped express power to refuse is useful. In particular, because the changes to accountability requirements in the bill are likely to result in fewer organisations requiring a DPO or SRI. We are also interacting with an increasingly diverse set of stakeholders, for example, codes and certification body representatives. Furthermore, our experience also shows that where requests are manifestly unfounded or excessive, the likelihood of challenge where we refuse to act is higher.

Part 2 – Digital verification services

Information Gateway

- **Clause 55 – Information disclosed by HM Revenue and Customs**

This clause relates to information disclosed by HM Revenue and Customs for the purposes of enabling a person to provide digital verification services. Subclause (5) provides a definition of personal data that differs

from other definitions found elsewhere in the bill. It is unclear if this is by design and we would suggest the clause is amended to bring it into line with other definitions of personal data.

- **Clause 56 – Code of practice about the disclosure of information**

This clause relates to the Secretary of State preparing and publishing a code of practice about the disclosure of information under section 54. Subclause (3) explains that a public authority must have regard to the code of practice when disclosing this information and goes on to define a public authority in subclause (11). However, this definition of a public authority differs from other definitions found elsewhere, such as Part 2 of the DPA 2018 (Chapter 2, Section 7). This is not necessarily problematic, but we would need assurance that the definition will not be cross-applied.

Part 3 – Customer data and Business data

- **Clause 74 – regulations under this Part**

This clause considers the provision for different areas of the legislation. Subclause (5) specifies that the Secretary of State or the Treasury must consult persons likely to be affected by the regulations and sectoral regulators with functions in relation to data holders likely to be affected by the regulations. We believe an explicit duty to consult the ICO should be set out in the drafting. The current reference to "sectoral" regulators creates ambiguity about whether this includes cross-economy regulators, such as the ICO.

Part 4 – Other provision about digital information

Privacy and electronic communications

- **Clause 79 – Storing information in the terminal equipment of a subscriber or user**

Clause 79 sets amendments to the Privacy and Electronic Communications Regulations 2003 (PECR) about storing and accessing information on the terminal equipment of users, including using 'cookies'.

In our view there are some minor drafting points which may result in unintended consequences. For example, the definition of the word "website" now inserted into Regulation 6B(8) and 6(7) is, in our view, an unnecessary overlap with the term 'Information Society Service' (ISS), and therefore may lead to confusion. The definition of an ISS is not in the data protection legislation and is used more broadly than just in PECR. It would be more appropriate for any changes to the definition to follow a broader review by the Government.

There may also be issues with the use of the term "automatically" in Regulation 6B. This is because the initial consent preferences may be set manually and in that sense may not be solely automatic, as is the case for current browser technology.

We note also that Regulation 6(2C), which is intended to ensure that organisations can benefit from an exemption from consent for software security updates, also contains safeguards to allow users to postpone or cancel the updates. In our view it is important for users to have a degree of knowledge and control over the installation of security updates. However, we also recognise that the current drafting could result in such updates being indefinitely postponed. This may have significant unintended consequences, for example, if organisations cannot roll out critical updates.

- **Clause 83 – Direct marketing for the purposes of democratic engagement**

This clause gives the Government power to make regulations to exempt political parties and others from the rules governing electronic communication in PECR, for the purposes of democratic engagement.

Whilst we support the Government's ambition to improve democratic engagement, this is an area in which there are significant potential risks to people if any future policy is not implemented very carefully.

Principally, we would want to ensure that the right to object to direct marketing is preserved in order to ensure that people do not receive unwanted calls. Whilst the right to object is set out in UK GDPR, Regulations 23 and 24 of PECR provide for the sender of the communication to have to identify themselves. Without this, people would not be able to exercise this right. It will therefore be important that this requirement is maintained. In our experience of regulating, people can find political direct marketing calls disturbing, particularly if the cause that they are being encouraged to support is one they disagree with.

Therefore, it will be important that there are rigorous safeguards around any future implementation of this policy. We welcome clause 83(6) which requires the Secretary of State to consider the effect any regulations would have on people's privacy, and 83(5) which specifies that the ICO is to be consulted on the development of any future regulations. It is also helpful that the regulations are subject to the affirmative resolution procedure in Parliament to ensure there will be proper scrutiny. We would be keen to bring our regulatory experience to bear at the earliest possible opportunity, and so would encourage the government to start any consultation process as soon as possible.

Trust services

- **Clause 90 – Recognition of overseas trust products**

This clause amends the eIDAS regulations in relation to overseas trust services.

Article 45A addresses the legal effects of overseas electronic signatures. This Article considers how the Secretary of State must be satisfied about the reliability of the products providing these services and in doing so having regard to the law in the other country or territory. It is unclear who has the expertise to make such an assessment (ie whether this is for the Secretary of State to determine or whether there is an expectation that ICO will undertake the assessment). This requires further clarification.

Part 6 – Final provisions schedules

Schedule 1 - Lawfulness of processing: recognised legitimate interests

General

We think it would be helpful if the explanatory notes could explicitly state that, in all the proposed new recognised legitimate interests, an assessment of necessity involves consideration of the proportionality of the processing activity. As our current guidance advises, a processing activity will not be necessary if it is not a targeted and proportionate means of achieving the stated purpose.

- **Disclosure for purposes of processing described in Article 6(1)(e)**

We suggest that this heading does not reflect the content of these new clauses and would be better expressed as "disclosures for the purposes of satisfying requests that a public authority has confirmed relate to its Article 6(1)(e) purposes" or similar. This would better reflect the purpose for which the disclosing data controller has to establish necessity.

We note the bill shifts responsibility for assessing whether a public authority needs personal data in order to perform its public task away from third party data controllers that might receive requests for such data from public authorities. It instead places that responsibility with the organisation seeking the information for the purposes of delivering the public task. We would seek to emphasise via guidance that public authorities requesting personal data from third parties should do so responsibly and ensure that they do not request more data than is necessary for their purposes. Otherwise they may find themselves non-compliant when they receive any data that they have requested unnecessarily. We note, however, that this clause does create an accountability gap. The requesting public authority will only become accountable when it receives any data, not when it requests it. Equally, we will only be able to exercise our powers to address any excessive processing of data and related harms to people at this later point.