Chapter 1- Reducing barriers to responsible innovation

1.2 Research Purposes

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

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

We welcome the principle of clarity or ease of navigation of the existing provisions for researchers conducting research. It is important to consider both legislative change and the provision of further ICO guidance as potential approaches when delivering such clarity. It is important that such changes are proportionate and do not lead to negative impacts on the rights and freedoms of data subjects, public trust or damage (alongside other changes) the EU adequacy agreement.

We would strongly advocate for health and care data to be included within the scope of the Digital Economy Act across the UK to support research activity in particular those research questions covering multiple topic areas including health. We accept that sufficient public engagement and safeguards would need to be in place to ensure the data were used appropriately.

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

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

Such a definition would need to be both sufficiently broad to be useful and provide clarity to researchers but narrow enough to avoid any negative consequences in respect of the rights and freedoms of data subjects, public trust or damage (alongside other changes) to the EU adequacy agreement.

Q1.2.3. Is the definition of scientific research currently provided by Recital 159 of the UK GDPR (‘technological development and demonstration, fundamental research, applied research and privately funded research’) a suitable basis for a statutory definition?

○ Yes

Please explain your answer, providing supplementary or alternative definitions of 'scientific research' if applicable.

Recital 159 is a suitable basis for a statutory definition but this will still need to be supported by guidance given that this is still a high level definition. Such guidance would need to avoid negative consequences in respect of the rights and freedoms of data subjects, public trust or damage (alongside other changes) to the EU adequacy agreement because the definition is, in practice, very broad.

Q1.2.4. To what extent do you agree that identifying a lawful ground for personal data processing for research processes creates barriers for researchers?

○ Somewhat disagree

Please explain your answer, and provide supporting evidence where possible, including by describing the nature and extent of the challenges.

In the case of Welsh Government research, identifying the lawful basis is not a barrier.

We are aware that Public bodies and Universities often rely on public interest legal basis (Article 6 (1)(e) of UK GDPR) or sometimes legitimate interest (Article 6 (1)(f))). Identifying the lawful basis in therefore not one of the largest barriers to undertaking research with the views from the research community on barriers to timely and effective research taking place being related to:

- Differing views on what constitutes 'anonymisation' of data so that it is no longer considered personal data - In the health data research space, the increasing development and standardisation of Trusted Research Environments (TREs) is beginning to bring some consistency to accepted approaches but further guidance to endorse such methods would be welcomed.
- Confusion between UK GDPR and common law duty of confidentiality – where consent is required under common law duty for disclosure of patient data but consent is often not a legal basis to be relied upon for research for purposes of UK GDPR. More detailed guidance on the relationship between UK GDPR and Common law duty in relation to research use of data would be beneficial

These two barriers often contribute to the concern by organisations that they might inadvertently breach data protection legislation and are, therefore, reluctant to share data even when the correct processes and arrangements are in place.

Q1.2.5. To what extent do you agree that clarifying that university research projects can rely on tasks in the public interest (Article 6(1)(e) of the UK GDPR) as a lawful ground would support researchers to select the best lawful ground for processing personal data?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

It seems highly unlikely that every University research project will be wholly in the public interest and a blanket approval may result in projects progressing where they have problems or unnecessarily impinge on data subjects' rights and freedoms. It will be an easier case to make in some areas than others – for example, medical research is more likely to be in the public interest than not. Potentially, this could also lead to personal data being processed for research purposes in instances where non-personal data would be sufficient to meet the aims of the research proposal.

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

○ Somewhat disagree

Please explain your answer, and provide supporting evidence where possible.

While clarity is welcomed this may be better achieved via improved guidance than a new lawful basis. For example, there is general concern in the biomedical research community that such a proposed change could have unintended negative consequences. There are already sufficient lawful basis that can be relied upon for the purposes of research and creating a new one could just add further confusion for the research community, particularly where they are already engaging with organisations and the public on their current understanding of the law. Further guidance on some key areas where interpretation of the law is unclear is likely to have a greater impact on facilitating timely research.

There is also the potential that the creation of a new legal basis might have negative impacts on public trust or damage (alongside other changes) the EU adequacy agreement which provides a benefit to UK research as part of wider collaborative projects.

Q1.2.7. What safeguards should be built into a legal ground for research?

The requirement for a robust data ethics assessment as part of the approvals process for any research project relying on these powers would be beneficial – along with clear requirements to ensure that data minimisation requirements are met, that non-personal data be used wherever possible, and that data subjects are informed about the use of their data and have clear processes to follow should they wish to be excluded or opt out at any point.

Specifically related to the research use of data, the 5 Safes framework championed by Health Data Research (HDR) UK is widely adopted by the health research community and should be the foundation for common approach to safeguards.

Q1.2.8. To what extent do you agree that it would benefit researchers to clarify that data subjects should be allowed to give their consent to broader areas of scientific research when it is not possible to fully identify the purpose of personal data processing at the time of data collection?

○ Somewhat disagree

Please explain your answer, and provide supporting evidence where possible.

Whilst this would be of benefit to researchers, it could have the effect of reducing transparency for data subjects, who would potentially be expected to provide consent for something that could not be described at all to them when that consent is sought. This could infringe on data subjects' rights and freedoms and may reduce an individual's willingness to consent for research uses in general. Potentially, this could be mitigated by allowing broad consent for certain types of research, rather than a broad consent for research in general.

Q1.2.9. To what extent do you agree that researchers would benefit from clarity that further processing for research purposes is both (i) compatible with the original purpose and (ii) lawful under Article 6(1) of the UK GDPR?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

Researchers would undoubtedly benefit from this; however, the rights of data subjects should be considered carefully, specifically how to ensure individuals understand how their data could be used and what is lawful and what is not lawful will be paramount.

Q1.2.10. To what extent do you agree with the proposals to disapply the current requirement for controllers who collected personal data directly from the data subject to provide further information to the data subject prior to any further processing, but only where that further processing is for a research purpose and it where it would require a disproportionate effort to do so?

○ Somewhat disagree

Please explain your answer, and provide supporting evidence where possible.

This will result in less transparency for data subjects and ultimately may dissuade people from providing their data in the first place if they are not confident they understand how it will be used. It will also remove their ability to opt out of future processing for research purposes they are not comfortable with and could negatively impact on their rights and freedoms.

A disproportionate effort test would vary between organisations who would likely consider various criteria – such as cost, resource, or time – differently when it comes to determining whether the burden is disproportionate or not. Whilst this is understandable (what is within the means of a larger organisation may not be within the means of a smaller one), it will inevitably result in substantial inconsistencies that data subjects may find difficult to understand, which in itself may reduce their willingness to share data with organisations.

Q1.2.11. What, if any, additional safeguards should be considered as part of this exemption?

Potential safeguards could include ensuring organisations have fully considered all the alternatives to using identifiable data under this exemption, requiring a full data ethics and data protection impact assessment that includes consideration of the potential impacts of reusing data without fully informing data subjects, and robust guidance on how to assess whether this would require disproportionate effort. Organisations should be required to document their reasoning and to make information available to data subjects as far as they are able and as is appropriate.

A major safeguard would be for organisations gathering data to ensure that wherever possible and appropriate, they have captured sufficient information about data subjects to ensure that they are in a position to easily notify people of an additional use of their data for research purposes. This data could be kept separately from any data being used for research purposes.

Further Processing

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

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

As the elements of the compatibility test are quite broad, it is inevitable that organisations will interpret them differently and some may take a more or less cautious approach than others. It is also likely to cause confusion for data subjects, as it is not fully clear what organisations may do with their data and what they may not – again, they may disagree with the assessment of compatibility.

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

○ Somewhat agree

Please explain your answer and provide supporting evidence where possible, including on:

○ What risks and benefits you envisage

○ What limitations or safeguards should be considered

Any measure designed to clarify how data can be reused will be beneficial for both data controllers and data subjects. Worked examples would increase the understanding of those who have to apply the test but also for data subjects – not just of uses which would meet the test but those that would not, as well as guidance on how to assess compatibility.

For incompatible uses that would rely on a public interest test, it would need to be clear what would allow this – for example, a local or national emergency could trigger the need to use data in different ways in order to protect individuals or to minimise wider impacts.

There are clear risks to public trust if any clarification is not handled sensitively plus potential negative impacts on the rights and freedoms of data subjects or damage (alongside other changes) the EU adequacy agreement

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

○ Somewhat agree

Please explain your answer and provide supporting evidence where possible, including on:

○ How you envisage clarifying when further processing can take place

○ How you envisage clarifying the distinction between further processing and new processing

○ What risks and benefits you envisage

○ What limitations or safeguards should be considered

'Further processing' is currently defined in ICO guidance as that which was unforeseen at the time the data was collected. This seems clear on the face of it; controllers should know in advance what data they want and why and to widen 'further processing' to give more leeway to this would not encourage proper scoping of the processing in advance. 'Further processing' is, by definition 'new processing' and the test is whether it is 'compatible' with the original processing. If there is doubt that the further processing involves sharing with another controller then clarification of that would be welcome, but there is a risk in removing the 'compatibility' aspect of further processing in that it could undermine the 'fair' and 'transparent' requirements of the original collection.

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

○ Strongly disagree

Please explain your answer and provide supporting evidence where possible, including on:

○ How you envisage clarifying when further processing can take place

○ How you envisage clarifying the distinction between further processing and new processing

○ What risks and benefits you envisage

○ What limitations or safeguards should be considered

Consent is quite clear under the current data protection regime; if the data subject did not consent to the further processing then it should not be carried out. Again, it comes down to the question of 'compatibility' and this is something for the controller to assess and defend on a case by case basis. This is an area that the potential negative impact on public trust and rights and freedoms of individuals are very likely to occur if such an approach to weakening consent is taken.

Legitimate Interests

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

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

As a public authority, Welsh Government's ability to rely on legitimate interests is limited. We would comment though that any list of legitimate interests would need to be clear and concise with no ambiguity.

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

○ Neither agree nor disagree

Please explain your answer, indicating whether and why you would remove any activities listed above or add further activities to this list.

As per the previous comment, these activities should ideally be clearly defined with unambiguous parameters. The list sets the sort of broad activities that would amount to legitimate interests, but defining it as (for example) "internal research and development purposes, or business innovation purposes" uses terminology that could be defined very widely with then potential negative impacts on the rights and freedoms of data subjects or public trust.

Q1.4.3. What, if any, additional safeguards do you think would need to be put in place?

The safeguards should be in the clarity and conciseness of the wording – i.e. that they are not open to abuse or exploitation.

Q1.4.4. To what extent do you agree that the legitimate interests balancing test should be maintained for children's data, irrespective of whether the data is being processed for one of the listed activities?

○ Strongly agree

Please explain your answer, and provide supporting evidence where possible.

Issues around safeguarding and the additional focus (including in legislation and the UN Convention of the Rights of a Child) on the rights of children suggest that the removing of any checks and balances in respect of children's data would be a move in the wrong direction. As such, the Welsh Government would wish to see the balancing test retained for children's data.

AI and Machine Learning

Q1.5.1. To what extent do you agree that the current legal obligations with regards to fairness are clear when developing or deploying an AI system?

○ Strongly disagree

Please explain your answer, and provide supporting evidence where possible.

Although the requirement to use data in a 'lawful, fair and transparent' way is described in the legislation, there is no statutory definition of what this means. In the presence of a wide spectrum of definitions, this causes considerable confusion both for those wanting to develop or deploy AI systems, and for data subjects, who have no reliable means to determine whether their data is being used in a reasonable way or not.

Q1.5.2. To what extent do you agree that the application of the concept of fairness within the data protection regime in relation to AI systems is currently unclear?

○ Strongly agree

Please explain your answer, and provide supporting evidence where possible

The multiplicity of definitions of fairness, from a variety of sources, make it difficult to determine what fairness means in relation to the development of AI systems – and is likely to cause significant confusion for data subjects, who also have no clear guidance on what constitutes a fair use of their data by AI systems, and indeed the rights in relation to the same.

Q1.5.3. What legislative regimes and associated regulators should play a role in substantive assessments of fairness, especially of outcomes, in the AI context?

Please explain your response.

There's a clear role for the ICO, CDEI and Equality and Human Rights Commission in this. Depending on the context (specifically the types of organisations and the nature of the data involved) other regulators or public authorities could also have a role, particularly where concepts of fairness and statutory requirements overlap – eg financial services, healthcare.

Q1.5.4. To what extent do you agree that the development of a substantive concept of outcome fairness in the data protection regime - that is independent of or supplementary to the operation of other legislation regulating areas within the ambit of fairness - poses risks?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible, including on the risks.

As the consultation states there are other avenues which could better assess this. The proposed AI governance framework could be more suited to this, however that is not yet in place.

Q1.5.5. To what extent do you agree that the government should permit organisations to use personal data more freely, subject to appropriate safeguards, for the purpose of training and testing AI responsibly?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible, including which safeguards should be in place.

Training and testing does not necessarily require identifiable data. Clearer guidance on the use of de-identified data should be explored further for this process. Ensuring that AI systems work accurately in use with real data is important and where it's necessary, it should be possible to do this provided there is no alternative.

Safeguards – data minimisation principles should apply, robust security and access measures in place.

Q1.5.6. When developing and deploying AI, do you experience issues with identifying an initial lawful ground?

Q1.5.7 When developing and deploying AI, do you experience issues with navigating re-use limitations in the current framework?

Q1.5.8 When developing and deploying AI, do you experience issues with navigating relevant research provisions?

Q1.5.9 When developing and deploying AI, do you experience issues in other areas that are not covered by the questions immediately above?

With no direct experience of developing AI the Welsh Government is unable to comment on questions Q1.5.6 to Q1.5.9.

Q1.5.10. To what extent do you agree with the proposal to make it explicit that the processing of personal data for the purpose of bias monitoring, detection and correction in relation to AI systems should be part of a limited, exhaustive list of legitimate interests that organisations can use personal data for without applying the balancing test?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible, including on:

○ the key benefits or risks you envisage

○ what you envisage the parameters of the processing activity should be

Ensuring AI systems function in a way which does not create bias for example is an important part of demonstrating the fairness and transparency of their use. This needs further work to demonstrate that this can be done in the interest of individual's rights and freedoms.

Q1.5.11. To what extent do you agree that further legal clarity is needed on how sensitive personal data can be lawfully processed for the purpose of ensuring bias monitoring, detection and correction in relation to AI systems?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

Given the sensitivities of special category data it is likely that such options should at least be explored in respect of any legislative changes to data protection in this area.

Q1.5.12. To what extent do you agree with the proposal to create a new condition within Schedule 1 to the Data Protection Act 2018 to support the processing of sensitive personal data for the purpose of bias monitoring, detection and correction in relation to AI systems?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

Given the sensitivities of special category data it is likely that such options should at least be explored in respect of any legislative changes to data protection in this area.

Q1.5.13 What additional safeguards do you think would need to be put in place?

This will depend on the details of the approach that is taken but even if there is a new condition within Schedule 1 of the Data Protection Act 2018 new guidance is likely to be needed plus the later proposals on removal of the need for a DPO in certain organisation and mandatory DPIAs would remove safeguards that would be essential in this area.

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

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible, including on:

○ The benefits and risks of clarifying the limits and scope of ‘solely automated processing’

○ The benefits and risks of clarifying the limits and scope of ‘similarly significant effects’

The current lack of clarity and applicable case law to guide these considerations makes these assessments difficult, so further clarity would be welcome. This would provide greater certainty for data controllers and processors, and clearer expectations from data subjects on what constituted automated decision making and how that affected their rights.

The risks are similar for both – too narrow a definition could impede the use of automated decision making for even low risk activities, or in areas where the public are largely used to a ‘computer’ making a decision for them – such as in applications for financial products like credit cards or insurance. Too wide a definition risks including processes that we cannot currently envisage as technology develops, and inappropriate uses would weaken public trust and impact on individual rights and freedoms.

Q1.5.15. Are there any alternatives you would consider to address the problem?

○ Don’t know

Please explain your answer, and provide supporting evidence where possible.

Q1.5.16. To what extent do you agree with the following statement: 'In the expectation of more widespread adoption of automated decision-making, Article 22 is (i) sufficiently future-proofed, so as to be practical and proportionate, whilst (ii) retaining meaningful safeguards'?

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible, on both elements of this question, providing suggestions for change where relevant.

This is a difficult question to answer given the constant change in technology and how this may then impact on individuals in ways that can not now be predicted. This should therefore be something that is kept under regular review.

Q1.5.17. To what extent do you agree with the Taskforce on Innovation, Growth and Regulatory Reform’s recommendation that Article 22 of UK GDPR should be removed and solely automated decision making permitted where it meets a lawful ground in Article 6(1) (and Article 9-10 (as supplemented by Schedule 1 to the Data Protection Act 2018) where relevant) and subject to compliance with the rest of the data protection legislation?

○ Strongly disagree

Please explain your answer, and provide supporting evidence where possible, including on:

○ The benefits and risks of the Taskforce’s proposal to remove Article 22 and permit solely automated decision making where (i) it meets a lawful ground in Article 6(1) (and, Articles 9 and 10, as supplemented by Schedule 1 to the Data Protection Act 2018) in relation to sensitive personal data, where relevant) and subject to compliance with the rest of the data protection legislation.

○ Any additional safeguards that should be in place for solely automated processing of personal data, given that removal of Article 22 would remove the safeguards

This would be a major erosion of data subjects existing rights, it could undermine public trust including on wider personal data uses, and could affect adequacy with the EU.

Q1.5.18. Please share your views on the effectiveness and proportionality of data protection tools, provisions and definitions to address profiling issues and their impact on specific groups (as described in the section on public trust in the use of data-driven systems), including whether or not you think it is necessary for the government to address this in data protection legislation.

No comments at this stage.

Q1.5.19. Please share your views on what, if any, further legislative changes the government can consider to enhance public scrutiny of automated decision-making and to encourage the types of transparency that demonstrate accountability (e.g. revealing the purposes and training data behind algorithms, as well as looking at their impacts).

No comments at this stage.

Q1.5.20. Please share your views on whether data protection is the right legislative framework to evaluate collective data-driven harms for a specific AI use case, including detail on which tools and/or provisions could be bolstered in the data protection framework, or which other legislative frameworks are more appropriate.

Data Protection is one vehicle to evaluate the potential harms of AI use, but it is not the only one – given that AI could also use anonymous, aggregated or statistical data, it could still cause harm. Data ethics, as well as equality and human rights concerns have a role to play in assessing the use of AI.

Data Minimisation and Anonymisation

Q1.6.1. To what extent do you agree with the proposal to clarify the test for when data is anonymous by giving effect to the test in legislation?

○ Strongly agree

Please explain your answer, and provide supporting evidence where possible.

This would provide further clarity for both data controllers and data subjects and would be welcome.

Q1.6.2. What should be the basis of formulating the text in legislation?

○ Recital 26 of the UK GDPR

Please explain your answer, and provide supporting evidence where possible.

This would provide further clarity for both data controllers and data subjects and would be welcome.

Q1.6.3 To what extent do you agree with the proposal to confirm that the re-identification test under the general anonymisation test is a relative one (as described in the proposal)?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

Re-identification needs to be based on whether data can be re-identified within their own organisation.

Q1.6.4. Please share your views on whether the government should be promoting privacy-enhancing technology, and if so, whether there is more it could do to promote its responsible use.

It could be difficult for government to promote specific products, however accreditation of products could build public trust. This may prove to be onerous so other alternatives such as codes of conduct or specific expectations could be helpful.

Innovative Data Sharing Solutions

Q1.7.1. Do you think the government should have a role enabling the activity of responsible data intermediaries?

○ Yes

Please explain your answer, with reference to the barriers and risks associated with the activities of different types of data intermediaries, and where there might be a case to provide cross-cutting support). Consider referring to the styles of government intervention identified by Policy Lab - e.g. the government's role as collaborator, steward, customer, provider, funder, regulator and legislator - to frame your answer.

In principle, however, more information on data intermediaries would be welcomed in order to fulyl respond. For example, what problems it is trying to solve and what understanding do we have on whether the public will really trust such an entity any more than other data sharing approaches.

Q.1.7.2. What lawful grounds other than consent might be applicable to data intermediary activities, as well as the conferring of data processing rights and responsibilities to those data intermediaries, whereby organisations share personal data without it being requested by the data subject?

Please explain your answer, and provide supporting evidence where possible, including on:

○ If Article 6(1)(f) is relevant, i) what types of data intermediary activities might constitute a legitimate interest and how is the balancing test met and ii) what types of intermediary activity would not constitute a legitimate interest

○ What role the government should take in codifying this activity, including any additional conditions that might be placed on certain kinds of data intermediaries to bring them within scope of legitimate interest

○ Whether you consider a government approved accreditation scheme for intermediaries would be useful

A key issues is whether such intermediary work is processing on behalf of a controller or not. If it is on behalf of a data controller then their lawful basis would apply but otherwise it is difficult without understanding the potential scenarios to suggest anything other than consent

Further Questions

Q1.8.1. In your view, which, if any, of the proposals in 'Reducing barriers to responsible innovation' would impact on people who identify with the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)?

All of the proposals have the potential to impact on any citizen and hence to have additional impacts on those with protected characteristics. Other than where specifically highlighted in the consultation questions, further processing and changes to consent would be areas of particular concern. While there is scope to better understand issues of equality and disadvantage this needs to be balanced with suitable safeguards and protections both generally and specifically in relation to special category data.

Q1.8.2. In addition to any of the reforms already proposed in ‘Reducing barriers to responsible innovation’ (or elsewhere in the consultation), what reforms do you think would be helpful to reduce barriers to responsible innovation?

No further comments at this stage.

Chapter 2 - Reducing burdens on businesses and delivering better outcomes for people

Privacy management programmes

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

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

In other areas of regulation, the UK has tended towards a "principles-based" rather than "rules-based" approach with some success and has avoided the negative effects of "box-ticking" regimes like SOX in the case of corporate governance, for example. However, the governance example also shows that principles-based alone is insufficient and not without risk – as the recent BEIS White Paper on "Restoring Trust in Audit and Corporate Governance" attests.

Having a rules-based accountability framework provides clarity and certainty about prescriptive requirements so aids compliance. However, there are aspects which may be onerous for organisations not processing much personal data or processing very low risk personal data, particularly smaller ones with limited resources for investment in their data protection infrastructure. There is a place for an assessment of risk to feature in the regulatory regime to ensure it remains proportionate, practicable and not overly burdensome.

An approach which encourages a proactive and systemic approach to the identification, management and mitigation of risks to data subjects' rights and freedoms which is suitable and proportionate is to be welcomed. However, a base-line minimum standard of controls may be needed and there will also need to be significant clarity and advice about how risk-based judgements are made.

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

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible and in particular:

○ Please share your views on whether a privacy management programme would help organisations to implement better, and more effective, privacy management processes.

○ Please share your views on whether the privacy management programme requirement would risk creating additional burdens on organisations and, if so, how.

Organisations may benefit from being required to develop and implement a risk-based privacy management programme to the degree such programmes are able to deliver a proportionate response to data protection risk. However, the focus of a risk-based approach must continue to be the risks to the rights and freedoms of data subjects and not the risk or, or to, the organisation. Where an organisation processes high volumes of high risk data, it is difficult to see what additional benefit is gained from a risk-based regime over the current rules-based regime.

If a risk-based privacy management programme can ensure an effective, principled and strong data protection culture and embed meaningful data protection practices which serve the data subject better, then this is to be welcomed. However, as above, such an approach is not without risk and may involve significant judgement by organisations as to what is an appropriate regime.

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

○ Neither agree nor disagree

Please explain your choice, and provide supporting evidence where possible.

○ Please share your views on which, if any, elements of a privacy management programme should be published in order to aid transparency.

○ What incentives or sanctions, if any, you consider would be necessary to ensure that privacy management programmes work effectively in practice.

The question posed is ambiguous. In certain scenarios where data is processed to a certain end then if a risk based approach results in an outcome that is beneficial to the data subject then the data subject will be content. However if a risk based approach results in their data being processed in a way they were not expecting then their rights and freedoms will not have been protected effectively. Different controllers are, inevitably, going to define risk in different ways depending on whether they regard their outcomes or data subject rights has having primacy. Clearly, it cannot be a ‘free for all’ and, ultimately, data processing is either lawful or it is not.

Data protection officer requirements

Q2.2.4. To what extent do you agree with the following statement: ‘Under the current legislation, organisations are able to appoint a suitably independent data protection officer’?

○ Somewhat agree

Please explain your choice, and provide supporting evidence where possible.

The current legislation does allow organisations to appoint a suitably independent data protection officer.

Q2.2.5. To what extent do you agree with the proposal to remove the existing requirement to designate a data protection officer?

○ Somewhat disagree

Please explain your answer, and provide supporting evidence where possible.

Again, this depends upon an organisation’s priorities. If it is cavalier with its risk then removing its data protection officer removes a gatekeeper of that risk.

The requirement of a mandatory data protection officer is a relatively recent development in terms of data protection but removing the requirement seems a backward step in terms of the protection of personal data – without sufficient time to really understand the impact on individuals in terms of mitigating data protection risk.

However, in the case of smaller public bodies, the mandatory requirement to have a Data Protection Officer can be burdensome and out of proportion to the risks to the rights and freedoms of data subjects arising from that organisation. There may be a case for making the requirement for a DPO the same for a public body as for a private sector organisation processing personal data, based on the volume and type of data processed. Other safeguards might be introduced instead, such as a periodic audit by the public body’s internal auditor to provide assurance on UK GDPR compliance.

Q.2.2.6. Please share your views on whether organisations are likely to maintain a similar data protection officer role, if not mandated.

We believe this will depend entirely on the culture of and commitment to data protection within an organisation. In the case of the private sector, it is likely to depend whether an organisations' customers understand and value high standards of data protection and the negative consequences on the organisation's reputation in the event of a critical data incident as well as organisations' appetite for risk and the cost of maintaining a [voluntary] regime.

Data protection impact assessments

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

○ Strongly agree

Please explain your answer, and provide supporting evidence where possible.

DPIAs have proved an effective tool in focussing minds at the start of any proposal to the requirements of ensuring any personal data is processed lawfully. They present a structured format where the personal data can be identified and justified by reference to the data protection principles. Without them personal data can become little more than an afterthought. There has also been insufficient time since their introduction to really understand the impact on individuals in terms of mitigating data protection risk.

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

○ Somewhat disagree

Please explain your answer, and provide supporting evidence where possible, and in particular describe what alternative risk assessment tools would achieve the intended outcome of minimising data protection risks.

DPIAs have proved an effective tool in focussing minds at the start of any proposal to the requirements of ensuring any personal data is processed lawfully. They present a structured format where the personal data can be identified and justified by reference to the data protection principles. Without them personal data can become little more than an afterthought. There has also been insufficient time since their introduction to really understand the impact on individuals in terms of mitigating data protection risk.

Prior consultation requirements

Q. 2.2.9 Please share your views on why few organisations approach the ICO for 'prior consultation' under Article 36 (1)-(3). As a reminder Article 36 (1)-(3) requires that, where an organisation has identified a high risk that cannot be mitigated, it must consult the ICO before starting the processing.

Please explain your answer, and provide supporting evidence where possible.

This may be due to ignorance, or else a fear the ICO will prevent them carrying out their intended processing. Within the Welsh Government, a formal process has been established to ensure all relevant proposals caught by Article 36 are presented to the ICO in a formal consultation format.

Q.2.2.10. To what extent do you agree with the following statement: ‘Organisations are likely to approach the ICO before commencing high risk processing activities on a voluntary basis if this is taken into account as a mitigating factor during any future investigation or enforcement action’?

○ Somewhat disagree

Please explain your answer, and provide supporting evidence where possible, and in particular: what else could incentivise organisations to approach the ICO for advice regarding high risk processing?

This would come down to the organisation’s attitude to risk and the recognition they are, in fact, processing personal data. If they believe the processing is high risk in terms of non-compliance but very low risk in terms of complaint or the data subject finding out then there would be little incentive to approach the ICO.

Record keeping

Q.2.2.11. To what extent do you agree with the proposal to reduce the burden on organisations by removing the record keeping requirements under Article 30?

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

The Welsh Government is already subject to records management requirements. Other organisations may see this as another opportunity to reduce costs at the expense of a clear data protection audit trail. Again, much comes down to the appetite for risk. The requirements should not be seen as a ‘burden’ and removing the obligation would be a backwards step.

Breach reporting requirements

Q.2.2.12. To what extent do you agree with the proposal to reduce burdens on organisations by adjusting the threshold for notifying personal data breaches to the ICO under Article 33?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible and in particular:

○ Would the adjustment provide a clear structure on when to report a breach?

○ Would the adjustment reduce burdens on organisations?

○ What impact would adjusting the threshold for breach reporting under Article 33 have on the rights and freedoms of data subjects?

Clarification of the breach reporting criteria would remove the uncertainty of when and what to notify to the ICO. Very often a breach can result in much internal dialogue over whether or not to report and often results in a report to err on the side of caution. For data subjects, it is something of an anomaly that the threshold for reporting is higher than for the ICO, meaning there are times when it is felt a data subject should be informed of a minor breach, if just out of courtesy, but which then raises the question of whether the ICO should be notified too. A reasonable and rational adjustment should not have any undue impact on the rights of data subjects.

Given the public nature of breach reporting, an overly sensitive approach can also lead to media scrutiny of public authorities over the quantity of fairly low risk breaches which can also lead to a negative impact on public trust.

Voluntary undertakings process

Q.2.2.13. To what extent do you agree with the proposal to introduce a voluntary undertakings process? As a reminder, in the event of an infringement, the proposed voluntary undertakings process would allow accountable organisations to provide the ICO with a remedial action plan and, provided that the plan meets certain criteria, the ICO could authorise the plan without taking any further action.

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

This could a useful and pragmatic proposal provided there is a mechanism for the ICO to confirm the plan has, in fact, been implemented by the authority, through some form of follow-up mechanism.

Q.2.2.14. Please share your views on whether any other areas of the existing regime should be amended or repealed in order to support organisations implementing privacy management requirements.

The Welsh Government has no strong views on other areas of the existing regime which might be amended or repealed to support organisation implementing privacy management requirements.

Q.2.2.15. What, if any, safeguards should be put in place to mitigate any possible risks to data protection standards as a result of implementing a more flexible and risk-based approach to accountability through a privacy management programme?

There is a clear trade-off and balance to be struck between proposals to replace current UK GDPR accountability standards with a more flexible approach. No controller can be flexible to the point of illegality so the flexibility offered should come with its own parameters that reflect the volume and sensitivity of the personal data it handles and the types of data processing the controller carries out.

Record-keeping

Q2.2.16. To what extent do you agree that some elements of Article 30 are duplicative (for example, with Articles 13 and 14) or are disproportionately burdensome for organisations without clear benefits?

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible, and in particular address which elements of Article 30 could be amended or repealed because they are duplicative and/or disproportionately burdensome for organisations without clear benefits.

The question is somewhat ambiguous; if elements of Article 30 duplicate elements of Article 13 and 14 then recording once would cover both obligations. An organisation with a clear understanding of the requirements will recognise this. Any extra ‘burden’ would appear negligible.

Breach reporting requirements

Q.2.2.17. To what extent do you agree that the proposal to amend the breach reporting requirement could be implemented without the implementation of the privacy management programme?

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

Much depends on the nature and scale of the breach reporting amendment. A controller will need some given parameters to determine when to notify but there is also a risk a detailed PMP would create a burden that did not previously exist. It is difficult to say more without more detail in this area.

Data protection officers

Q.2.2.18. To what extent do you agree with the proposal to remove the requirement for all public authorities to appoint a data protection officer?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

In the case where a public body is very small and processes minimal personal data and/or very little personal data of high risk, the burden of appointing a data protection officer may be disproportionate and difficult to achieve effectively or meaningfully. Such bodies will probably rely on the provisions which allow for an external DPO, or are likely to give the DPO role to a non-expert official already responsible for other aspects of public administration within the organisation. In both cases, it is hard to see how the mandated appointment of a DPO contributes effectively to the achievement of high standards of data protection. In terms of value for money from the use of public funds, the costs of a mandated requirement where there would, otherwise, be justification for such an appointment do not represent good value for public money.

The application of a risk-based approach to the appointment of a DPO for public bodies, in line with the same approach use by other organisations processing personal data, would deliver a more proportionate and reasonable data protection regime in the public sector. However, such a change might risk the loss of some trust and confidence by the public in the processing of their data by public bodies, if this were perceived as a weakening of public sector data protection.

Q.2.2.19. If you agree, please provide your view which of the two options presented at paragraph 184d(V) would best tackle the problem.

Please provide supporting evidence where possible, and in particular:

○ What risks and benefits you envisage

○ What should be the criteria for determining which authorities should be required to appoint a data protection officer

Neither option is considered better than the other. Given other organisations appoint a DPO based on criteria which reflect the volume and type of data they use, it is difficult to see what different set of criteria would be set for a public body given the current criteria reflect the risk to the data subject.

Q2.2.20 If the privacy management programme requirement is not introduced, what other aspects of the current legislation would benefit from amendments, alongside the proposed reforms to record keeping, breach reporting requirements and data protection officers?

The Welsh Government has no strong views on other areas of the current legislation which might be amended or repealed in this area. However, it would welcome more detailed advice and guidance than is currently provided by either the ICO or the EDPB on:

- the role and responsibilities of a data protection officer and how they should be fulfilled;
- the nature of “monitoring compliance”, how this is done and what this actually means.

In other areas of public life, the UKG has embraced the “three lines of defence” approach (used by the UKG risk management, internal audit and project management communities). The UKG might

innovate and take the lead in encouraging the application of this approach to assurance in the case of "monitoring compliance" with UK GDPR

Also, while the current UK GDPR is clear on the need for a DPO to be independent and impartial within an organisation, there is little guidance or commentary on what constitutes a suitable information governance (IG) and data protection regime. In some cases, IG teams are being led by the organisation's DPO, although this makes the DPO partly responsible for the organisational and technical measures they are then required to monitor. In other cases, DPOs are operating in functions separate from and independent of the IG function, to allow the DPO to monitor the operations of that function as part of monitoring compliance. Guidance on appropriate IG frameworks would assist organisations to structure and management their data protection functions appropriately.

The DPO is required to have protected reporting lines to the senior leadership of an organisation in order to raise concerns and flag non-compliance with the UK GDPR. However, unlike other assurance functions, like internal audit in the public sector, there is no requirement for the DPO to report formally on the monitoring of compliance at any level or on any frequency. This might also be addressed in more detailed guidance from the ICO.

Subject Access Requests

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

Please provide supporting evidence where possible, including:

○ What characteristics of the subject access requests might generate or elevate costs

○ Whether vexatious subject access requests and/or repeat subject access requests from the same requester play a role

○ Whether it is clear what kind of information does and does not fall within scope when responding to a subject access request

It has been the Welsh Government's experience that the introduction of data subject access requests under GDPR has not been any more time consuming than SARs under DPA98. The burden under both regimes is much the same and is based around those requesters that ask for 'all' their personal data with no parameters. It is difficult to brand such requests 'vexatious' (in an FOI sense) if the data subject genuinely does not know what data we are processing on them and wants to find out; poor records management processes should not be used as an excuse to deny an individual their rights. A well-structured and clear DSAR generally does not present a burden.

However, for FOI public authorities there can be an issue where a wide ranging freedom of information request inadvertently captures the requester's own personal data. In our experience, data subjects often confuse which regime applies when they are asking for data and requests for information frequently combine both organisational and personal data. There can be a burden in identifying and distinguishing which information falls under which regime and then dealing with them accordingly.

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

○ Neither agree nor disagree

Please explain your answer, providing supporting evidence where possible, including on what, if any, measures would make it easier to assess an appropriate threshold.

The ‘Manifestly unfounded’ threshold is not so much ‘too high’ as too poorly defined. There is little in GDPR itself to define this and the ICO guidance is restrictive. In the absence of clear case law it remains very much of an unknown quantity. Clear statutory guidance would help though it is also important to note that ‘manifestly unfounded’ is an ‘exemption’ to all the GDPR data subject rights (rectification etc.) not just subject access.

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

○ Somewhat disagree

Please explain your answer, and provide supporting evidence where possible, including on:

○ Which safeguards should apply (such as mirroring Section 16 of the Freedom of Information Act (for public bodies) to help data subjects by providing advice and assistance to avoid discrimination)

○ What a reasonable cost limit would look like, and whether a different (ie. sliding scale) threshold depending on the size (based on number of employees and/or turnover, for example) would be advantageous

The rights of access under the Freedom of Information Act and DSARs are different. The right to personal data is underpinned by an obligation on controllers to know what personal data they are processing; if it is not necessary then it should be deleted. If there is an approach that DSARs can be rejected along the lines of FOI s12 then it would appear there is non-compliance on the part of the controller in knowing the personal data it holds – to tell X that it would take over 24 hours to confirm whether an organisation is processing personal data and then to locate it would prima facie conflict with the fundamental legal requirements of processing personal data.

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

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible, including what a reasonable level of the fee would be, and which safeguards should apply.

There is a case in the sense a fee would deter any spurious requests and would help cut down on ‘inadvertent’ DSARs (e.g. when they are mixed with an FOI request in the example above) but the removal of the fee has not resulted in a marked increase in DSARs made to the Welsh Government. The DPA98 required data subjects to pay a fee for twenty years so re-introducing it would not be a radical step but it would be perceived as a backwards one in terms of data rights.

Q2.3.5. Are there any alternative options you would consider to reduce the costs and time taken to respond to subject access requests?

○ Yes

Please explain your answer, and provide supporting evidence where possible.

There could be an option to expand or clarify the ‘excessive’ provision and allow controllers to refuse on that basis once the appropriate advice and assistance has been provided. This, though, should be justified on a case-by-case basis and not the objective FOI standard of 24 hours work.

Privacy and electronic communications

Q2.4.1. What types of data collection or other processing activities by cookies and other similar technologies should fall under the definition of 'analytics'?

Anonymous statistical information on use of a website or service such as referral sites, visit duration and other categories generally accepted as audience measurement.

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

○ Somewhat agree

Please explain your choice, and provide supporting evidence where possible, including what safeguards should apply.

Anonymous cookies which capture data on the performance of a website or application are a useful method for improving the quality and delivery of websites and services. Those limited to a single website or application which do not capture individual preferences may be acceptable. Consent should always be sought for those aimed at targeting or identifying users after they have ended their session and across other websites.

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

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible, including what circumstances should be in scope and what, if any, further safeguards should apply.

Users and Controllers have a joint interest in improving the technical standards and operation of sites and services. Many users of sites and services have a low level of understanding of the purpose and use of cookies. They may dismiss or refuse consent for all purposes without understanding that the use of this data could improve a service or site they rely upon. Removing consent requirements, particularly where data is anonymised, could be considered. However, if we take enabling the use of video as an example, this may benefit the user in accessing a wider range of content but at the same time could be considered intrusive if this is to enable advertising or third party content. A sound ethical framework would be required.

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

○ Strongly disagree

Please explain your answer, and provide supporting evidence where possible, including how organisations could comply with the UK GDPR principles on lawfulness, fairness and transparency if PECR requirements for consent to all cookies were removed.

Users of sites and services have an expectation that their data is used ethically and in a way that respects their privacy. A lack of user understanding as to the purpose and use of cookies doesn’t present as a valid reason to remove their wholesale ability to manage their data.

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

Guides could be useful but not at the expense of sound legislative controls, rather they should support rather than replace.

Q2.4.6. What are the benefits and risks of requiring websites or services to respect preferences with respect to consent set by individuals through their browser, software applications, or device settings?

The benefits are that it removes the need for repetitive actions by the user to set their privacy preferences and to navigate and understand the range of tools that websites or services deploy. A potential disadvantage is that some sites or services may not operate without some consents, preventing the user from accessing the site or service. This may not be immediately apparent to the user and cause frustration and confusion.

Q2.4.7. How could technological solutions, such as browser technology, help to reduce the volume of cookie banners in the future?

Browser technologies could remove the need for vast number of different and often confusing tools deployed by websites and services to capture cookie consent. Users are expected to be given options as to how their data is used in a simple and consistent manner.

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

The 'soft opt-in' in relation to direct marketing activities

Q2.4.9. To what extent do you agree that the soft opt-in should be extended to non-commercial organisations? See paragraph 208 for description of the soft opt-in.

○ Somewhat agree

This seems reasonable as long as organisations do not rely on a soft opt-in if they obtained a marketing list from a third party – this should require specific consent.

Nuisance and fraudulent calls

Q2.4.10. What are the benefits and risks of updating the ICO's enforcement powers so that they can take action against organisations for the number of unsolicited direct marketing calls 'sent'?

Q2.4.11. What are the benefits and risks of introducing a 'duty to report' on communication service providers?

Q2.4.12. What, if any, other measures would help to reduce the number of unsolicited direct marketing calls and text messages and fraudulent calls and text messages?

Q2.4.13. Do you see a case for legislative measures to combat nuisance calls and text messages?

○ Don't know

If yes, what measures do you propose and why?

If no, please explain your answer, and provide supporting evidence where possible.

Q2.4.14. What are the benefits and risks of mandating communications providers to do more to block calls and text messages at source?

Q2.4.15 What are the benefits and risks of providing free of charge services that block, where technically feasible, incoming calls from numbers not on an 'allow list'? An 'allow list' is a list of approved numbers that a phone will only accept incoming calls from.

The Welsh Government have no comments on this section at this stage.

Bringing PECR's enforcement regime into line with the UK GDPR and Data Protection Act

Q2.4.16. To what extent do you agree with increasing fines that can be imposed under PECR so they are the same level as fines imposed under the UK GDPR (i.e. increasing the monetary penalty maximum from £500,000 to up to £17.5 million or 4% global turnover, whichever is higher)?

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

There could be benefits in terms of transparency and consistency

Q2.4.17. To what extent do you agree with allowing the ICO to impose assessment notices on organisations suspected of infringements of PECR to allow them to carry out audits of the organisation's processing activities?

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

There could be benefits in terms of transparency and consistency

Q2.4.18. Are there any other measures that would help to ensure that PECR's enforcement regime is effective, proportionate and dissuasive?

○ Don't know

If yes, what measures do you propose and why?

Use of personal data for the purposes of democratic engagement

Q2.5.1. To what extent do you think that communications sent for political campaigning purposes by registered parties should be covered by PECR's rules on direct marketing, given the importance of democratic engagement to a healthy democracy?

Please explain your answer, and provide supporting evidence where possible.

Q2.5.2. If you think political campaigning purposes should be covered by direct marketing rules, to what extent do you agree with the proposal to extend the soft opt-in to communications from political parties?

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

Q2.5.3. To what extent do you agree that the soft opt-in should be extended to other political entities, such as candidates and third-party campaign groups registered with the Electoral Commission? See paragraph 208 for description of the soft opt-in

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

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

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

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

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

Further Questions

Q2.6.1. In your view, which, if any, of the proposals in 'Reducing burdens on business and delivering better outcomes for people', would impact on people who identify with the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)?

All of the proposals have the potential to impact on any citizen and hence have additional risk for those with protected characteristics. Any benefits needs to be weighed against those risk

Q2.6.2. In addition to any of the reforms already proposed in 'Reducing burdens on business and delivering better outcomes for people', (or elsewhere in the consultation), what reforms do you think would be helpful to reduce burdens on businesses and deliver better outcomes for people?

Chapter 3 - Boosting trade and reducing barriers to data flows

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

○ Somewhat agree

Please explain your answer and provide supporting evidence if possible.

Welsh Government recognise that adequacy is a non-devolved issue, and would welcome any simplification of rules, however whilst recognising that in general the impact to Wales would be equal to that of the rest of the UK, there some specific issues for us.

On Adequacy - we would seek re-assurance that the changes proposed to Enhancing Public Safety (para 323) would not impact on EU Adequacy. The EU remains one of the priority adequacy agreements for Wales and any impact on the current adequacy arrangements would negatively impact Wales.

Creating a scalable, flexible adequacy regime

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

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

In progressing the programme of adequacy assessments of other countries, we are supportive of this but would require re-assurance that consultation with officials would happen on priorities and progress. Each Devolved Government will have its own priority list of countries to pursue which must be considered if this programme is to benefit the whole of the UK eg Africa ,which would support our Wales for Africa programme. However maintaining adequacy with the EU would be our first priority.

In assessing sectors or territories as being adequate, this would increase complexity and potentially cause confusion. Whilst we are aware that there are some agreements in place at the moment, these tend to be in heavily regulated areas such as Finance. In introducing a more sectoral approach, we run the risk of creating complexity and confusion for the data exporter in determining whether the business they are exporting to sits within an agreed sector or territory.

Q3.2.3. To what extent do you agree with the proposal to strengthen ongoing monitoring of adequacy regulations and relax the requirement to review adequacy regulations every four years?

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

We have some concerns with regards to the proposed four stage procedure for new adequacy agreements. From the consultation documentation is it not clear whether this procedure would be the same for sectoral / territorial decisions as well. Step c, the recommendation stage, does not account for sectoral agreements that may impact on devolved competence, such as an agreement for educational or health data for example. There is no mention of consultation with or approval from Ministers of Devolved Governments, which would be necessary if it impacted on devolved responsibilities.

Also in step c, the validity of the consultation with the ICO would be dependent on the extent of ICO reform (also a matter in this consultation).

With regard to strengthening the on-going monitoring of adequacy agreements, this would be welcomed, but must relate to any sectoral / territorial agreements as well. As for the intention to **relax the requirement to review adequacy regulations every four years**, we would require further information on what this meant. If it means removing formal assessment all together this would be seen as a significant risk. We would prefer there to remain a formal assessment at regular as backstop and provided that the continuous monitoring was adequate this would be a less burdensome process than currently.

Redress requirements

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

○ Somewhat agree

Please explain your choice, and provide supporting evidence where possible.

We agree in principle in bringing in clarity on judicial and administrative redress, however this does depend on the proposals for the ICO reform to ensure that our administrative redress process would be fit for purpose, and the process for assessing other countries regulatory bodies on their ability to provide effective administrative redress.

Alternative Transfer Mechanisms

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

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

On Alternative Transfer mechanisms – we welcome in principle the aim of providing clear guidance that are more flexible and adaptable.

Q3.3.2. What support or guidance would help organisations assess and mitigate the risks in relation to international transfers of personal data under alternative transfer mechanisms, and how might that support be most appropriately provided?

Any guidance should make it clear what the process of thinking should be for any organisation with standard templates where possible to help consistency and transparency

Reverse transfers exemption

Q3.3.3. To what extent do you agree that the proposal to exempt 'reverse transfers' from the scope of the UK international transfer regime would reduce unnecessary burdens on organisations, without undermining data protection standards?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

Agree that reducing the burden for data processors based in the UK would be welcome, however any exemption from UK GDPR would have to be allowed only on data that has purely been processed

and returned. If the data set had been added to with any other data, then that new data should fall under UK GDPR. This would hinge on the clarity of definitions of processor / controller relationships.

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

The issue of Devolved competence may also be applicable in relation to any sectorial agreements that are made by companies, or where they insert clauses such as data storage (which is devolved) into their bespoke contracts. Allowing organisations to create their own agreements without specific knowledge of devolved issues and competencies could risk them ignoring devolution.

Adaptable transfer mechanisms

261. The government is considering whether to empower organisations to create or identify their own alternative transfer mechanisms in addition to those listed in Article 46 of the UK GDPR. Such a change would benefit organisations with complex data transfer requirements, which could, for example, design and use bespoke contracts to enable safe international transfers. This would supplement the existing options for transfers in Article 46 of the UK GDPRQ3.3.4. To what extent do you agree that empowering organisations to create or identify their own alternative transfer mechanisms that provide appropriate safeguards will address unnecessary limitations of the current set of alternative transfer mechanisms?

○ Somewhat disagree

Please explain your answer, and provide supporting evidence where possible.

We believe there is a risk in allowing organisations the flexibility to create their own alternative transfer mechanisms without the regulatory approval. This approach would be most utilised by larger organisations that have the knowledge and resources to explore these options and therefore put business in Wales at a disadvantage as the vast majority of business are SMEs and would not necessarily have the resource to utilise this option.

https://gov.wales/longitudinal-small-business-survey-2019-html

Q3.3.5 What guidance or other support should be made available in order to secure sufficient confidence in organisations' decisions about whether an alternative transfer mechanism, or other legal protections not explicitly provided for in UK legislation, provide appropriate safeguards?

Any guidance should make it clear what the process of thinking should be for any organisation with standard templates where possible to help consistency and transparency

Q3.3.6. Should organisations be permitted to make international transfers that rely on protections provided for in another country's legislation, subject to an assessment that such protections offer appropriate safeguards?

○ No

Please explain your answer, and provide supporting evidence where possible.

Allowing organisations to create their own, without regulatory approval will depend on the proposed ICO reforms as the proposed change to remove the need for a DPO or the DPIA, there would not be a named individual in the organisation who would be responsible for carrying out the impact assessments.

Allowing organisations to assess the third countries data privacy laws and deciding to transfer data outside of agreed alternative transfer mechanisms seems to infer that adequacy decision would be delegated to organisations. This would run the risk of some organisations deeming them adequate, and some not, creating confusion, not clarity. Again this option would only be applicable to larger organisations that have the resources, disadvantaging the majority of Welsh businesses.

A power to create new alternative transfer mechanisms

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

○ Somewhat disagree

Please explain your answer, and provide supporting evidence where possible.

This could have devolved competence implications and should not be done without consultation/agreement of Devolved Governments where there are devolved competence concerns.

Q3.3.8. Are there any mechanisms that could be supported that would benefit UK organisations if they were recognised by the Secretary of State?

○ No

Please explain your answer, and provide supporting evidence where possible.

This could have devolved competence implications and should not be done without consultation/agreement of Devolved Governments where there are devolved competence concerns.

Certification Schemes

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

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

Not enough information to make a judgement at this time.

Q3.4.2. To what extent do you agree that allowing accreditation for non-UK bodies will provide advantages to UK-based organisations?

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

Need more information in order to answer this question. How accountable will they be to UK data subjects? Will they be governed by UK or third country law? Introducing competition into a regulatory environment does not necessarily lead to improved protections – it could just drive down standards and drive up risk for example.

Q3.4.3. Do you see allowing accreditation for non-UK bodies as being potentially beneficial for you or your organisation?

○ Neither agree nor disagree

Please explain the advantages and risks that you foresee for allowing accreditation of non-UK bodies.

Not enough information to make a judgement at this time.

Q3.4.4. Are there any other changes to certifications that would improve them as an international transfer tool?

○ Neither agree nor disagree

Not enough information to make a judgement at this time.

Derogations

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

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

Further Questions

Q3.6.1. The proposals in this chapter build on the responses to the National Data Strategy consultation. The government is considering all reform options in the round and will carefully evaluate responses to this consultation. The government would welcome any additional general comments from respondents about changes the UK could make to improve its international data transfer regime for data subjects and organisations.

Q3.6.2. In your view, which, if any, of the proposals in 'Boosting Trade and Reducing Barriers to Data Flows' would impact on people who identify with the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)?

All of the proposals have the potential to impact on any citizen and hence to have additional impacts on those with protected characteristics. The main impact on any citizen would be if the safeguards are sufficient and the risk are just that much greater in terms of special category data.

Q3.6.3. In addition to any of the reforms already proposed in 'Boosting Trade and Reducing Barriers to Data Flows' (or elsewhere in the consultation), what reforms do you think would be helpful to make the UK's international transfer regime more user-friendly, effective or safer?

Chapter 4 - Delivering better public services

Q4.2.1. To what extent do you agree with the following statement: ‘Public service delivery powers under section 35 of the Digital Economy Act 2017 should be extended to help improve outcomes for businesses as well as for individuals and households’?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

The aims seem reasonable in principle, although we are not entirely clear how this would work in practice and how it would be ensured this does not lead to negative impacts on the rights and freedoms of data subjects, public trust or damage (alongside other changes) to the EU adequacy agreement.

We would strongly advocate the inclusion across the UK of health and care into Digital Economy Act Public service delivery powers. This acts as a significant barrier to achieving the potential benefits from the PSD powers and undermines the ability of public sector organisations to integrate services for the benefit of individual well-being

Use of Personal Data in the COVID-19 Pandemic

Q4.3.1. To what extent do you agree with the following statement: ‘Private companies, organisations and individuals who have been asked to process personal data on behalf of a public body should be permitted to rely on that body’s lawful ground for processing the data under Article 6(1)(e) of the UK GDPR’?

○ Neither agree nor disagree

Please explain your answer, providing supporting evidence where possible.

It is unclear why they would not be able to rely on that lawful ground; there does not appear to be any reason in the legislation why a private company cannot perform a task in the public interest. The dual nature of 6(1)e (public interest or public task) can cause confusion and guidance may help controllers and data subjects understand this lawful basis more clearly.

Q4.3.2. What, if any, additional safeguards should be considered if this proposal were pursued?

It is unclear why there would need to be safeguards over and above the private company identifying and justifying the task in the public interest they are pursuing and then identifying the necessity of the processing.

Processing health data in an emergency

Q4.3.3. To what extent do you agree with the proposal to clarify that public and private bodies may lawfully process health data when necessary for reasons of substantial public interest in relation to public health or other emergencies?

○ Somewhat agree

Please explain your answer, providing supporting evidence where possible.

The existing legislation provides a proper basis for such a response although additional guidance (particularly reflecting on the lessons learned during the COVID-19 pandemic) would be helpful to ensure that during an emergency, swift decision making can occur to support data sharing to save live based on clarity around the legislation. It is also important to ensure some data sharing activity is possible as part of recovery from an emergency, to ensure public authorities can continue to support

the well-being of individuals. We accept this will need some consideration into the definition of "recovery".

Q4.3.4. What, if any, additional safeguards should be considered if this proposal were pursued?

Not relevant where any changes are restricted to improved guidance.

Building Trust and Transparency

Q4.4.1. To what extent do you agree that compulsory transparency reporting on the use of algorithms in decision-making for public authorities, government departments and government contractors using public data will improve public trust in government use of data?

○ Somewhat agree

Please explain your choice, and provide supporting evidence where possible.

This builds on some existing principles around Open Government and Open Data. This would improve transparency, particularly around decision making, policy making and operational delivery, and would be welcome.

Q4.4.2. Please share your views on the key contents of mandatory transparency reporting.

The following should be considered:

- The purpose of the algorithm
- What data is being used (and its source)
- The code itself
- Any DPIA, ethics assessment or other considerations made before it was used.

Q4.4.3. In what, if any, circumstances should exemptions apply to the compulsory transparency reporting requirement on the use of algorithms in decision-making for public authorities, government departments and government contractors using public data?

Areas such as defence or national security and some areas of crime detection may require this. Publishing details of algorithms in testing/development might be difficult to manage as they are unfinished products. Guidance would be welcome on the expectation and exemptions if this is taken forward.

Processing in the 'substantial public interest'

Q4.4.4. To what extent do you agree there are any situations involving the processing of sensitive data that are not adequately covered by the current list of activities in Schedule 1 to the Data Protection Act 2018?

○ Neither agree nor disagree

Please explain your answer and provide supporting evidence where possible, including on:

○ What, if any, situations are not adequately covered by existing provisions

○ What, if any, further safeguards or limitations may be needed for any new situations

This is difficult to answer without an indication of what scenarios are felt to be insufficiently covered by the existing provisions. Further information should be provided to inform any decisions on this.

Q4.4.5. To what extent do you agree with the following statement: ‘It may be difficult to distinguish processing that is in the substantial public interest from processing in the public interest’?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

The difference between substantial public interest and public interest is not well defined and open to interpretation – by both data controllers and data subjects. The lack of case law and clear examples compounds this.

Q4.4.6. To what extent do you agree that it may be helpful to create a definition of the term 'substantial public interest'?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible, including on:

○ What the risks and benefits of a definition would be

○ What such a definition might look like

○ What, if any, safeguards may be needed

An overly broad definition could negatively impact on data subjects’ rights and thus jeopardise adequacy. However, an overly narrow definition could further impede processing and could also have negative effects on data subjects’ rights.

Q4.4.7. To what extent do you agree that there may be a need to add to, or amend, the list of specific situations in Schedule 1 to the Data Protection Act 2018 that are deemed to always be in the substantial public interest?

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible, including on:

○ What such situations may be

○ What the risks and benefits of listing those situations would be

○ What, if any, safeguards may be needed

Any need would need to be evidenced on the basis of shortcomings evidenced by practical examples and then assessed in terms of why they were not included in the original drafting; The Data Protection Act is three years old and practical cases are still emerging.

Clarifying rules on the collection, use and retention of biometric data by the police

Q4.4.8. To what extent do you agree with the following statement: ‘There is an opportunity to streamline and clarify rules on police collection, use and retention of data for biometrics in order to improve transparency and public safety’?

○ Somewhat agree

Please explain your answer, providing supporting evidence where possible.

Greater transparency is welcomed where it builds public trust and confidence in the use of biometric data by the police in a fair and proportionate manner. However, this will need to come with safeguards and ethical considerations will need to be put in place. For this reason, streamlining and clarifying the rules in this space will be helpful.

Public Safety and National Security

Q4.5.1. To what extent do you agree with the proposal to standardise the terminology and definitions used across UK GDPR, Part 3 (Law Enforcement processing) and Part 4 (Intelligence Services processing) of the Data Protection Act 2018?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

Agree to the principles laid out in the consultation, the more aligned the language between both sets of regulations the reduction in likelihood of misinterpretation. However, understanding and guidance as to which regulation is being applied must be unambiguous to ensure the person is aware of which set of regulations being applied and support consistency of use.

Strengthening data security and sharing opportunities is important and offering the ability to share information more easily between Law Enforcement and Intelligence Services would be welcomed, however the guidance or protocols that would underpin are key**,** it is important that proper safeguards are in place to ensure to prevent misuse of data.

Further Questions

Q4.6.1. In your view, which, if any, of the proposals in 'Delivering Better Public Services' would impact on people who identify with the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)?

All of the proposals have the potential to impact on any citizen and hence to have additional impacts on those with protected characteristics. The main impact on any citizen would depend whether safeguards remain sufficient. The risks are just that much greater in terms of special category data. There is a balance to be struck between the beneficial use of data (to improve services) and the risks to individuals and the extent to which it is possible to mitigate those risks.

Q4.6.2. In addition to any of the reforms already proposed in 'Delivering Better Public Services' (or elsewhere in the consultation), what reforms to the data protection regime would you propose to help the delivery of better public services?

We have no additional comments at this stage.

Chapter 5 - Reform of the Information Commissioner's Office

Q5.2.1.To what extent do you agree that the ICO would benefit from a new statutory framework for its objectives and duties?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

There is always a benefit in ensuring an organisation has clear objectives and this move would bring it into line with other UK Regulators.

Q5.2.2. To what extent do you agree with the proposal to introduce an overarching objective for the ICO with two components that relate to upholding data rights and encouraging trustworthy and responsible date use respectively?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

Again, we recognise this would bring it into line with other UK Regulators but would caution that the objectives should allow the ICO to maintain its independence.

Q5.2.3. Are there any alternative elements that you propose are included in the ICO's overarching objective?

○ No

Please explain your answer, and provide supporting evidence where possible.

The ICOs overarching objective is considered to be sufficient.

Growth and innovation duty

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

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

Along with the ICO, we believe this will serve to enhance the clarity of purpose and accountability of the future ICO for stakeholders such as the Welsh Government**.**

Competition duty

Q5.2.5. To what extent do you agree with the proposal to introduce a duty for the ICO to have regard to competition when discharging its functions?

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

Whilst not holding strong views either way, the Welsh Government notes the need to ensure this is consistent with, and reflected in, parallel work to align the duties and powers of other regulators participating in the Digital Regulation Cooperation Forum.

Collaboration and enhanced information sharing gateways

Q5.2.6. To what extent do you agree with the proposal to introduce a new duty for the ICO to cooperate and consult with other regulators, particularly those in the DRCF (CMA, Ofcom and FCA)?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

The Welsh Government recognises the benefits in ensuring regulators work in a joined up way where required.

Q5.2.7. Are there any additional or alternative regulators to those in the Digital Regulation Cooperation Forum (CMA, Ofcom and FCA) that the duty on the ICO to cooperate and consult should apply to?

○ Don't know

Please explain your answer, and provide supporting evidence where possible.

Q5.2.8. To what extent do you agree with the establishment of a new information sharing gateway between relevant digital regulators, particularly those in the DRCF?

○ Neither agree nor disagree

Although data sharing in this way can be beneficial, it is important to ensure all participating regulators take the privacy and data protection rights of the data subject into account.

Q5.2.9. Are there any additional or alternative regulators to those in the DRCF (ICO, CMA, Ofcom and FCA) that the information sharing gateway should include?

○ Don't know

Please explain your answer, and provide supporting evidence where possible.

Public safety duty

Q5.2.10. To what extent do you agree with the government's proposal to introduce specific language recognising the need for the ICO to have due regard to public safety when discharging its functions?

○ Neither agree nor disagree

Please explain your answer and provide supporting evidence where possible.

We would need to see the detail of the proposal to be able to comment with any confidence; whilst salutatory in principle, the privacy of the data subject also needs to be protected.

Statement of strategic priorities

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

○ Somewhat disagree

Please explain your answer, and provide supporting evidence where possible.

Again, the detail of the proposal will be important, but the Welsh Government believes it is important, for both government and the ICO, that the ICO has complete independence when it comes to the final sign-off of any such strategic priorities. In addition, it is important that devolved administrations should have involvement in the development of strategic priorities.

The ICO's international role

Q5.2.12. To what extent do you agree with the proposal to require the ICO to deliver a more transparent and structured international strategy?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

We agree this would help the ICO prioritise its activities in light of its expanding remit in these areas following the UK's exit from the European Union**.**

Q5.2.13. To what extent do you agree with the proposal to include a new statutory objective for the ICO to consider the government's wider international priorities when conducting its international activities?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

We agree this would help the ICO prioritise its activities in light of its expanding remit in these areas following the UK's exit from the European Union.

Governance Model and Leadership

Q5.3.1. To what extent do you agree that the ICO would benefit from a new governance and leadership model, as set out above?

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

We cannot add to the ICO's own comments on this point.

Appointments processes

Q5.3.2. To what extent do you agree with the use of the Public Appointment process for the new chair of the ICO?

○ Somewhat disagree

Please explain your answer, and provide supporting evidence where possible.

This would result in the ICO having a different model to that adopted by other economic regulators and would, therefore, give the ICO a constitution less independent from government than that of other economic regulators, despite its role in overseeing the public sector and government.

Q.5.3.3. To what extent do you agree with the use of the Public Appointment process for the non-executive members of the ICO's board?

○ Somewhat disagree

Please explain your answer, and provide supporting evidence where possible.

We believe this proposal presents a risk to the ICO’s independence. Given the range of other proposals, including the issues of safeguards and protections highlighted in the consultation itself, we believe a strong, independent (and seen to be independent) ICO is one of the strongest safeguards across the full range of data protection issues and the proposed changes.

Q5.3.4. To what extent do you agree with the use of the Public Appointment process for the new CEO of the ICO?

○ Somewhat disagree

Please explain your answer, and provide supporting evidence where possible.

We believe this proposal presents a risk to the ICO’s independence. Given the range of other proposals, including the issues of safeguards and protections highlighted in the consultation itself, we believe a strong, independent (and seen to be independent) ICO is one of the strongest safeguards across the full range of data protection issues and the proposed changes.

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

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

We cannot add to the ICO’s own views on this.

Accountability and Transparency

Q5.4.1. To what extent do you agree with the proposal to strengthen accountability mechanisms and improve transparency to aid external scrutiny of the ICO's performance?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

As a regulator of other public authorities it would be useful to see how the regulator itself is performing.

Q5.4.2. To what extent do you agree with the proposal to introduce a requirement for the ICO to develop and publish comprehensive and meaningful key performance indicators (KPIs) to underpin its annual report?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

As a regulator of other public authorities it would be useful to see how the regulator itself is performing. Introducing KPIs to the ICO's performance would give a clear indication of that performance.

Q5.4.3. To what extent do you agree with the proposal to require the ICO to publish the key strategies and processes that guide its work?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

We believe this would aid transparency within the ICO.

Q5.4.4. What, if any, further legislative or other measures with respect to reporting by the ICO would aid transparency and scrutiny of its performance?

○ Don't know

Please explain your answer, and provide supporting evidence where possible.

Q5.4.5. Please share your views on any particular evidence or information the ICO ought to publish to form a strong basis for evaluating how it is discharging its functions, including with respect to its new duties outlined above.

Clear objectives and deliverables and KPIs to show progress

Independent review

Q5.4.6. To what extent do you agree with the proposal to empower the DCMS Secretary of State to initiate an independent review of the ICO's activities and performance?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

As the ICO themselves have the power to independently review the performance of other authorities, this would add independent accountability to the ICO itself. However, the terms of any independent review will be critical, to ensure the independence and impartiality of the ICO is not undermined.

Q5.4.7. Please share your views on what, if any, criteria ought to be used to establish a threshold for the ICO's performance below which the government may initiate an independent review.

We believe these should be in line with the ICO's own threshold criteria for independently reviewing other authorities.

Codes of Practice and Guidance

Q5.5.1. To what extent do you agree with the proposal to oblige the ICO to undertake and publish impact assessments when developing codes of practice, and complex or novel guidance?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

As data protection is an area open to interpretation this proposal would be useful to ensure the ICO's codes of practice are balanced and reasonable and to aid understanding of the outcomes the ICO is seeking to achieve through each code of practice.

Q5.5.2. To what extent do you agree with the proposal to give the Secretary of State the power to require the ICO to set up a panel of persons with expertise when developing codes of practice and complex or novel guidance?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

We agree with the proposal to give the Secretary of State this power but with the caveat that the persons with expertise are selected for their knowledge and expertise and are seen as independent experts rather than, for example, lobbyists with an agenda.

Q5.5.3. To what extent do you agree with the proposal to give the Secretary of State a parallel provision to that afforded to Houses of Parliament in Section 125(3) of the Data Protection Act 2018 in the approval of codes of practice, and complex and novel guidance?

○ Strongly disagree

Please explain your answer, and provide supporting evidence where possible.

We believe this risks undermining the independence of the ICO and damaging the neutrality and impartiality of its guidance and codes of practice. Given the range of other proposals, including the issues of safeguards and protections highlighted in the consultation itself, we believe that a strong, independent (and seen to be independent) ICO is one of the strongest safeguards across the full range of data protection issues and the proposed changes.

Q5.5.4. The proposals under this section would apply to the ICO's codes of practice, and complex or novel guidance only. To what extent do you think these proposals should apply to a broader set of the ICO's regulatory products?

○ Strongly disagree

Please explain your answer, and describe alternative or supplementary criteria if appropriate.

We believe this risks undermining the independence of the ICO and damaging the neutrality and impartiality of its guidance and codes of practice. Given the range of other proposals, including the issues of safeguards and protections highlighted in the consultation itself, we believe that a strong, independent (and seen to be independent) ICO is one of the strongest safeguards across the full range of data protection issues and the proposed changes.

Q5.5.5 Should the ICO be required to undertake and publish an impact assessment on each and every guidance product?

○ Don't know

Please explain your answer, and provide supporting evidence where possible.

Complaints

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

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

The Welsh Government does not find the ICO's current approach particularly disproportionate.

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

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

The ICO already does this to an extent. Formalising the process would bring clarity but we believe the data controller should be able to direct a complainant directly to the ICO where an internal review by the data controller is unlikely to produce a different outcome or change in the data protection practice being complained about.

Q5.6.3. To what extent do you agree with the proposal to require data controllers to have a simple and transparent complaints-handling process to deal with data subjects' complaints?

○ Strongly agree

Please explain your answer, and provide supporting evidence where possible.

This would be of benefit to both controller and data subject in terms of clarity and transparency of process.

Please also indicate what categories of data controllers, if any, you would expect to be exempt from such a requirement.

A data subject should have a right of redress against any controller subject to the caveat set out in 5.6.2

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

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

It is difficult to comment without seeing the detail of the proposal and the criteria around which complaints will not be taken forward. There is a risk that, if a controller sees the ICO will not be investigating a complaint, then they will not do so themselves, leaving the data subject without the right for redress other than legal action via the courts.

Enforcement Powers

Q5.7.1. To what extent do you agree that current enforcement provisions are broadly fit for purpose and that the ICO has the appropriate tools to both promote compliance and to impose robust, proportionate and dissuasive sanctions where necessary?

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

The ICO's enforcement powers appear broadly fit for purpose, albeit not currently used extensively.

Q5.7.2. To what extent do you agree with the proposal to introduce a new power to allow the ICO to commission technical reports to inform investigations?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible, including:

○ Whether there are any other risks or benefits you can see in this proposal

○ If you foresee any risks, what safeguards should be put in place

Any investigation would benefit from the appropriate specialist or technical input. The caveat is that the specialists are independent and chosen for their knowledge and expertise and would be seen as impartial.

Q5.7.3. Who should bear the cost of the technical reports: the organisation (provided due regard is made to their financial circumstances) or the ICO?

The organisation that requests the report or believes it is necessary.

Q5.7.4. If the organisation is to pay, what would an appropriate threshold be for exempting them from paying this cost?

We do not have a view at this stage

A power to compel witnesses to answer questions at interview

Q5.7.5. To what extent do you agree with what the government is considering in relation to introducing a power which explicitly allows the ICO to be able to compel witnesses to attend an interview in the course of an investigation?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible. In particular, please give your views on any benefits or risks you envisage and what measures could mitigate these risks.

Data losses or breaches can be devastating for the data subject. If a witness can help with an investigation to ascertain what happened then this could ensure co-operation and could aid a satisfactory conclusion as well as contributing to public trust and confidence in the regulatory process.

Q5.7.6. To what extent do you agree with extending the proposed power to compel a witness to attend an interview to explicitly allow the ICO to be able to compel witnesses to answer questions in the course of an investigation?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible. In particular, please give your views on:

○ Any benefits or risks you envisage

○ What, if any, additional safeguards should be considered

Data losses or breaches can be devastating for the data subject. If a witness can help with an investigation to ascertain what happened then this could ensure co-operation and could aid a satisfactory conclusion. However, such a power would need to be in line with similar ones in other areas.

Amending the statutory deadline for the ICO to issue a penalty following a Notice of Intent

Q5.7.7. To what extent do you agree with the proposal to amend the statutory deadline for the ICO to issue a penalty following a Notice of Intent in order to remove unnecessary deadlines on the investigations process?

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

Whilst deadlines can be prohibitive they can also provide focus. Controllers need certainty so it would be unfair to have a potential penalty notice hanging over them indefinitely.

Q5.7.8. To what extent do you agree with the proposal to include a 'stop-the-clock' mechanism if the requested information is not provided on time?

○ Somewhat agree

Please explain your answer, and provide supporting evidence where possible.

This would ensure the ICO has sufficient time to investigate in the face of procrastination by the controller.

Enhancing the ICO's accountability regarding investigations

Q5.7.9. To what extent do you agree with the proposal to require the ICO to set out to the relevant data controller(s) at the beginning of an investigation the anticipated timelines for phases of its investigation?

○ Somewhat disagree

Please explain your answer, and provide supporting evidence where possible.

This would aid transparency of the process but would only be of immediate benefit to the parties involved.

Biometrics Commissioner and Surveillance Camera Commissioner

Q5.8.1. To what extent do you agree that the oversight framework for the police's use of biometrics and overt surveillance, which currently includes the Biometrics Commissioner, the Surveillance Camera Commissioner and the ICO, could be simplified?

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

The proposal is not controversial but there is not enough detail to comment beyond the ICO's own comments.

Q5.8.2. To what extent do you agree that the functions of the Biometrics Commissioner and the Surveillance Camera Commissioner should be absorbed under a single oversight function exercised by the ICO?

○ Neither agree nor disagree

Please explain your answer, and provide supporting evidence where possible.

The proposal is not controversial but there is not enough detail to comment beyond the ICO's own comments.

Further Questions

Q5.9.1. In your view, which, if any, of the proposals in 'Reform of the Information Commissioner's Office' would impact on people who identify with the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)?

All of the proposals have the potential to impact on any citizen and hence to have additional impacts on those with protected characteristics. The main impact on any citizen would be if the safeguards a strong independent regulator provides were weakened and the risks to data subjects' rights and freedoms are just that much greater in terms of special category data.