Domestic Data Protection team
DCMS
100 Parliament Street
London
SW1A 2B

Castle House
6 Castle Drive
Carnegie Campus
Dunfermline
KY11 8GG
LP – 4, Dunfermline 2

T: 0845 601 8855
W: www.scottishwater.co.uk

19th November 2021

Data: a new direction

Scottish Water welcomes the opportunity to comment on the Department for Digital, Culture, Media & Sport's open consultation on proposals to reform the data protection regime.

Scottish Water is Scotland's statutory water and sewerage authority. Every day we deliver 1.53 billion litres drinking water; and remove 1.08 billion litres of wastewater which we treat and return safely to the environment. Our services support 2.57 million households and 152,916 business premises across Scotland. We turn over nearly £1.3bn and we employ around 4,000 people. It is publicly owned and answers to the Scottish Government.

In delivering our services we hold and process large amounts of data, some of which is personal data. We are committed to protecting the data and information we hold on our employees, customers, contractors and members of the public. We recognise our responsibility, as a public utility, to safeguard their interests and we seek to earn and retain the confidence and trust of all those with whom we deal.

As some of the areas of consultation are not particularly germane to our business, we have confined our response largely to matters that we believe affect the delivery of our services.

Chapter 1 – Reducing Barriers to Responsible Innovation

We welcome the proposal in Section 1.4. (60) to create a limited, exhaustive list of legitimate interests for which organisations can use personal data without applying the balancing test. We agree that it would give more confidence to allow the processing of personal data without unnecessary reliance on consent, which can cause considerable

uncertainty due to deliberations about whether it was freely given, specific, informed and unambiguous and has not been withdrawn.

We often have deliberations over whether consent is needed or if other bases for processing are more suitable. The two legitimate interest definitions included in section 61 are particularly relevant regarding research and innovation projects designed to improve services to the public and would help us to maintain an up-to-date database, stop duplication and assure accuracy.

We also believe that a list of legitimate interests would be useful in relation to reporting crime and dealing with security issues. This would save time and administrative resources by removing the need to carry out the balancing exercise and help individuals to understand how their personal data might be used in similar ways by organisations for the public good.

Also, we would find it particularly useful to have legitimate interests as a legal basis for processing personal data for the purpose of improving the safety of services that our organisation provides or delivers and for innovations relating to reducing carbon emissions.

We welcome the proposals in Section 1.5 about reusing personal data which would clarify when to do so would be regarded as being in public the interest.

Scottish Water's general statutory powers are wide but we do not generally share personal data on research projects. We do get a lot of requests for data but most of it has all personal data removed. However, where that is not feasible, it would be useful to rely on legitimate interest as the basis for processing.

The proposal in Section 1.6 (121) to put in law what constitutes anonymisation is welcomed. We have had many issues with people claiming they can be identified when it would take a great deal of effort to be able to do so or the likelihood of someone doing so is very small.

We favour Option (a) as we believe that commercial organisations already have a reasonable understanding of the intention behind Recital 26 of UK GDPR. The alternative test based on the Explanatory Report seems unnecessarily complicated and inconsistent with the objective of reducing barriers to responsible innovation.

The proposals in Section 1.7 relating to innovative data sharing solutions support data sharing which is secure and easy and talks about responsible data intermediaries. Our view is that personal data must be adequately protected and if it is accessible to data intermediaries, data subjects know what they are being used for. Data intermediaries may be valuable for small and medium organisations who do not have expertise in data protection and privacy law and we cautiously welcome the proposal to encourage their development. However, organisations with sufficient in-house knowledge to keep up to date with developments in IT and data protection issues should be slow to outsource the handling of personal data. In principle, the proposals would cut down on bureaucracy and help some organisations but could create new risks for organisations unless strict regulation of intermediaries could be relied on.

Chapter 2 – Reducing Burdens on Business and Delivering Better Outcomes for People

We believe that proposals in Section 2 (156) relating to an accountability framework are already covered by what we do. We recognise that accountability is important to give individuals trust in the use that their data might be put to by public sector and commercial organisations and to give them confidence to allow more data sharing while will benefit of society as a whole.

Section 2 (160) proposes the removal of existing requirements to designate a data protection officer. Our view is that there should be someone at executive level responsible for overseeing data protection within large organisations. Although the title is not particularly important, “data protection officer” helps give focus to the idea of someone with an independent view who can deal with data protection issues and who helps keep them on the organisations’ agenda. We are not convinced that the requirements of the accountability framework really maintain sufficient independence. In larger organisations, it may be useful to appoint another person or persons to deal with accountability for low-risk data to allow someone higher up in the organisation to deal with potential high-risk processing and data breaches. The current regime allows that to happen.

Section 2 (167) would remove the requirement for organisations to undertake a data protection impact assessment for processing likely to result in a high risk to individuals and would let organisations adopt different approaches to identify and minimise data protection risks that better reflect their specific circumstances. The proposals envisage a privacy management programme mitigating risks associated with this. While we have, in effect, a privacy management programme already in place through our PIA/DPIA processes, we would welcome this change as it would enable us to tailor our work to focus on the key data privacy and protection risks to the organisation.

More generally, we would hope that regular independent reviews of businesses that handle high risk personal data would be undertaken to ensure their privacy management programmes are robust.

The services that we provide do not generally involve processing high risk personal data. Where that does happen (e.g., in relation to maintaining priority services registers and some HR functions), we adopt a data minimisation policy.

The current requirements for a full DPIA where there is any likelihood of risk to individuals are onerous. While it is helpful to do some form of risk assessment at the start of planning a new process or purchasing new software, where that process identifies ways to mitigate the risk and introduce adequate safeguards, a prescriptive DPIA which may involve irrelevant considerations should not always be necessary.

The ability to tailor the privacy management programme would assist in focussing the risk assessment objectives and make it easier for organisation to take actions to safeguard personal data based on circumstances relevant to their business.

Section 2 (177) proposes to remove record keeping requirements under Article 30. We would welcome this as the current requirements are very detailed and difficult to keep up to date. We acknowledge that as part of the accountability framework a record of some sort would need to be kept but would welcome freedom to decide the format. A form of record keeping that identifies what personal data is being processed and for what purpose is necessary for the operation of the concept of data protection by design and default. Where the record keeping process identifies that any risk of harm to individuals or breach of data processing or privacy rights from processing data is low, less detailed information could be recorded than is currently required under Article 30 for the Single Inventory.

Section 2 (180) considers whether to change the threshold for reporting a data breach to the ICO so that organisations must report a breach unless the risk to individuals is not material. We would certainly agree that the ICO should be encouraged to produce guidance and examples of what constitutes a ‘non-material’ risk. This would reduce over reporting and allow the ICO to focus resources on more serious cases.

We would also support a requirement for the complainant to attempt to resolve their complaint directly with the relevant data controller before lodging a complaint with the ICO.

We think there needs to be guidance on what to do when a complaint becomes lengthy and unresolvable. Could there be an opportunity for organisations to refer complaints to the ICO themselves for a ruling?

A complaint process similar to the review process followed by freedom of information legislation may reduce the burden on the ICO resources and give organisations and individuals the opportunity to resolve issues directly. Recourse to ICO could still be necessary to maintain independence for example where dealing with employees’ personal data where the bargaining powers are not in balance.

We welcome proposals in Section 2 (188) to introduce a fee regime and to look at adopting similar rules to freedom of information legislation relating to vexatious requests.

Clear guidance on what constitutes a vexatious request and what kind of data is applicable for release under a subject access request would be very welcome.

We have had requests for many years’ worth of data which have taken great amounts of effort and cost to respond to. Requests for data and information are often fishing exercises to obtain documents to help with a claim or are used by some claimants and their lawyers as a bargaining tactic. The concept of “discovery” in court procedures is different in Scotland but this use of data protection legislation is being used to replicate some of the system operated by courts in England and Wales. We believe that, if the Scottish Government wished to introduce similar procedures, they would legislate for it.

While SW rarely charge fees for FOI requests, it would be useful to have a way of recovering some costs when dealing with requests that involve large amounts of time

and resources or are clearly unreasonable. We would welcome a regime for SARs, similar to the FOI process, which encourages the clarification of requests and internal review of decisions prior to a complaint being referred to the ICO. The proposals could reduce the time spent by organisations on locating data and help individuals to obtain a response that is more relevant to the purpose of the request.

Chapter 3 – Boosting Trade and Reducing Barriers to Data Flow

We would welcome changes to reduce barriers to data transfers and moves to explore legislative change to ensure that the suite of transfer mechanisms available to UK organisations is clear, flexible and provides the necessary protections for personal data.

We believe the current procedures required for transfer of personal data outwith the EU are complicated and time consuming to implement. Simplification of the new Risk Transfer Tool proposed by the ICO would be welcome.

A risk-based approach to international transfers would be better. We see this particularly in relation to cloud-based services. An internationally accepted certification process would remove the need for each customer to repeat the same assessments in relation to subjects such as the applicability local law and the local enforcement regime. Controllers could then concentrate their risk assessment on the circumstances that are relevant to the personal data being processed by their organisation.

Chapter 4 – Delivering Better Public Services

We are supportive of proposals that would clarify that private companies, organisations and individuals who have been asked to process personal data on behalf of a public body need not identify a separate lawful ground. This would be of considerable assistance to Scottish Water.

Clarification of how 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 would be welcome and would have saved a lot of debate and head scratching relating utilities compiling registers to identify customers with special requirements.

It is important that Scottish Water, as a public sector organisation, can enable data and information to be used to innovate and achieve benefits for the public. However, it is also important that people understand how their data is used and can be confident that high risk processing is fair and appropriate. There is a move to require organisations to have a clear ethical use policy, compliance with which is monitored and reported.

We would welcome clarification on whether substantial public interest can be used as the legal basis of processing data sets involving personal data, particularly where sharing with other public bodies. The public task legal basis for processing allows us to collect data for meeting our core statutory obligations. A list of legitimate interests, similar to that proposed in section 1 for innovation, could form a legal basis for sharing specified categories of personal data with other public bodies and utilities would be useful.

This would also benefit society by reducing costs currently spent on collecting, duplicating and storing similar data sets.

Proposals to clarify that further processing for a different purpose may be permitted when it safeguards a substantial public interest would be of benefit to us.

Similar considerations apply to delivering better public services as apply to research and innovation, particularly where the risk to individuals is low and sharing data would be in line with public expectations of improved public services. We believe that updating the UK GDPR and/or Data Protection Act 2018 would be preferable to relying on the Digital Economy Act to enable public sector data sharing. The data protection legislation is more user-friendly and more widely encountered and understood by both individuals and businesses. The Digital Economy Act has significant limitations on current powers for data sharing among public sector organisations and unwieldy provisions for obtaining new powers.

Chapter 5 – Reform of ICO's Office

We have no firm views on this section but would hope that some of the other proposals would enable the ICO might be able to spend more time monitoring what organisations do rather than dealing with minor complaints.

As a heavily regulated organisation, we see it as important to maintain the independence of the Information Commissioner's Office as a regulator. The proposed reforms outlined in other sections, such as reducing the threshold for reporting data breaches and introducing procedures similar to FOI legislation for reviewing decisions could result in better allocation of ICO resources. The implementation of the proposed overarching objective for the ICO with two key elements, (i) upholding data rights and (ii) encouraging trustworthy responsible use of data, makes sense. This would give public sector organisations and other innovators more confidence to share data.

We believe that the UK could benefit from a less administrative approach to data management if the ICO has a statutory duty to balance the rights of individuals and the need to innovate and improve public services by sharing personal data where appropriate.

As a public body based in Scotland, we come under the Freedom of Information (Scotland) Act and the remit of the Scottish Information Commissioner for FOI but the UK ICO for data protection. We realise that is due to devolved responsibilities to the Scottish Government but should be recognised when talking about the ICO cooperating and consulting with other regulators. It may be a barrier to the ICO carrying out the overarching role relating to information that is envisaged.

Rob Mustard

Director of Digital