Appendix A

Summary of the DCMS consultation Data: New Direction

The DCMS (the Department for Digital, Culture, Media and Sport) have published a consultation document entitled Data: new direction. Their stated aim is to amend UK GDPR, DPA 2018 and PECR 2003, so that it aligns with ambitions around growth and innovation and becomes easier to understand. Consultation on the new proposals is open until the 19 November.

The document sets out principles which guide their proposals.

a) The UK's data protection regime should create a net benefit for the whole of the UK, unlocking new economic opportunities both at home and abroad, and keeping our society safe and secure
b) The UK's data protection regime should be future-proofed with a responsive framework that enables responsible innovation and a focus on privacy outcomes that avoids imposing any rules today that become obsolete as the technological landscape evolves
c) The UK's data protection regime should deliver a high standard of data protection for citizens whilst offering organisations flexibility in determining how to comply most effectively
d) Organisations that comply with the UK's current regime should still be largely compliant with our future regime, except for only a small number of new requirements
e) The government's approach to data protection should actively take into account the benefits of responsible use of personal data, while proactively maintaining public trust in such uses
f) Effective, risk-based and preventative supervision is critical to realising a pro-growth and trusted data regime, and the ICO's world-leading status as the UK's independent data protection regulator should be sustained

The proposals don't deviate from current key elements of UK GDPR such as data processing
principles, rights and the mechanisms around monitoring and enforcement however there are significant proposals across a range of areas, and these are summarised for each chapter below.

Chapter 1 – 'Reducing barriers to responsible innovation'

This chapter contains proposals to reduce barriers to using data for secondary research purposes and to further processing including by third parties. There is consideration given to the role regulations need to take to recognise AI including the significance of fairness, safeguarding and public trust. There are proposals to developing further legislation around data anonymisation.

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

The changes proposed may be significant for the Council, organisations will remain liable for investigation and the same level of fines under the old regime

should they fail to meet the data protection standards of the UK GDPR. Proposals include

- Reducing the burdens under the accountability framework, taking a risk-based approach based on the Canadian Privacy Management Programmes, organisations would still be required to have in place risk management processes, including the processes which allow for the identification, assessment and mitigation of data protection risks.
- There are also proposals to reduce burdens of DPIAs and Breach Reporting but against this there also proposals to introduce the government is considering whether to introduce a new voluntary undertakings process, similar to Singapore's Active Enforcement regime.
- In recognition of organisations capacity to process SARs there are proposals to introduce a fee, create a cost limit and threshold for response similar to FOI.
- Changing the rules around the collection of data around website cookies.
- Reducing the rules around political campaigning to give greater freedom.

Chapter 3 – 'Boosting trade and reducing barriers to data flows'

UK will maintain the existing framework for international data transfers, only permitting the transfer of personal data across borders when additional legal safeguards are met, such as the presence of a data adequacy agreement, the use of standard contract clauses, organizational arrangements, codes of conduct and specific derogations. The UK however will consult to allow for the greater use of some of these safeguards to suit more data transfer situations and looking to embed additional flexibility in the system so the UK can respond to new international transfer methods.

Chapter 4 – 'Delivering better public services'

This chapter partly responds to barriers encountered during Covid-19.

- It seeks to reflect the importance of third parties processing data for the public sector, by proposing to give them the same lawful basis to process as the public body. The Government however does not plan to introduce a general requirement that would compel disclosure of personal information to law enforcement or intelligence agencies.
- Extend the use of the Digital Economy Act
- Provide clarity 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.
- The government proposes introducing compulsory transparency in the reporting on the use of algorithms in decision-making for public authorities, government departments and government contractors using public data.
- Making the meaning of substantial public interest clearer which is a lawful basis for processing special category data. The proposal is whether to add a definition to the legislation, add new situations to the list set out in the Data Protection Act 2018 (DPA), or amend the existing situations.
- Streamlining and clarifying the rules on the collection, use and retention of biometric data by the police.

- Clarifying the rules on joint controllership in the DPA to facilitate improved cross-sector working, in particular the joint operational activity between law enforcement and national security partners.
- They are also consulting on removing the requirement for a DPO but organisations would need to document roles and responsibilities. Two alternative options are presented:
    - Allowing public authorities to follow the same approach as private sector organisations for determining whether it is necessary to appoint a DPO, i.e. a DPO would only be required if the authority's core activities consist of large-scale monitoring of data subjects or large-scale use of sensitive data or criminal convictions data.
    - Retain the requirement, but limit its scope to authorities meeting certain criteria, e.g. size of body, volume of data and aspects of the processing, such as whether it is for the purpose of making decisions affecting the data subjects.

Chapter 5 – 'Reform of the Information Commissioner's Office'

There is concern that UK GDPR does not provide the ICO with a sufficiently clear framework within which to operate and they want to empower the ICO unlock the power of data not just protect rights. Reforms suggested include changes to ICO's constitution and objectives to bring it in line with other regulators some of these proposals include:

- A new, statutory framework for the ICO to have greater account in economic growth, innovation and competition and for the ICO to deliver a more structured and transparent international strategy.
- New power for the Secretary of State for DCMS to prepare a statement of strategic priorities to inform how the ICO sets its own regulatory priorities.
- Reform the structure of the ICO to include an independent board and a chief executive officer. The board would be led by a chair with non-executive directors. The chief executive officer would have responsibility for the running of the organisation, while answering to the board.
- Importantly for the Council there is a proposal that complainants will be required to attempt to resolve their complaints directly with the relevant data controller before lodging a complaint with the ICO. This is aimed at reducing the burden on the ICO and the number of vexatious complaints received.
- As such proposals also include a requirement on data controllers to have a simple and transparent complaints-handling process in place to deal with data subject complaints.