A&L Goodbody

GENERAL DATA PROTECTION

Data Protection: *a new direction*

On 10 September 2021, the UK Government's Department for Digital, Culture, Media and Sport ('**DCMS**') published their proposed reforms to the UK's data protection regime in a document entitled, *Data: A new direction*.

The DCMS Consultation closed on 19 November 2021 and the Government is expected to publish its response to the consultation in Spring 2022, heralding significant changes to the current data protection framework.

5 MIN READ

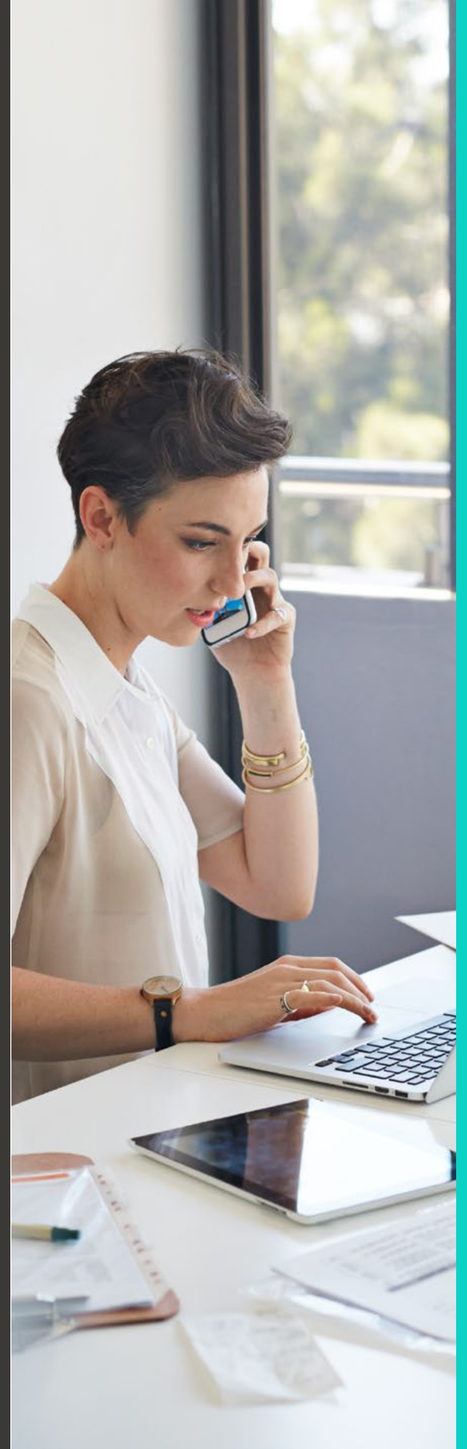
Background

The DCMS Consultation is the first step in the Government's plan to deliver on the National Data Strategy, which is underpinned by the government's desire to 'secure a pro-growth and trusted data regime in the UK.'

The Government aims to create a data protection regime that will:

- support vibrant competition and innovation to drive economic growth
- maintain high data protection standards without creating unnecessary barriers to responsible data use
- keep pace with the rapid innovation of data-intensive technologies
- help innovative businesses of all sizes to use data responsibly without undue uncertainty of risk (both UK and Internationally), and
- ensure the ICO is equipped to regulate effectively in an increasingly data-driven world

The Consultation focuses on 5 key areas including: reducing barriers to responsible innovation, reducing burdens on businesses and delivering better outcomes for people, boosting trade and reducing barriers to data flows, delivering better public services and the reform of the ICO.



Chapter 1 - Reducing barriers to responsible innovation

The Consultation recognises that data protection regimes require active interpretation and application to new and emerging technologies. The UK's data protection regime should be adaptable enough to be interpreted quickly in order to fit the fast-changing world of data-driven technologies. In this aspect, the Consultation asked for the public's views relating to data protection law surrounding: research specific provisions, legitimate interests, deployment of AI systems, data minimization and anonymization and innovative data sharing solutions.

Clarifying requirements when processing for research purposes

The Government is concerned that the lack of regulatory clarity regarding the requirements when processing for research purposes creates uncertainty for business and stifles the effective use of data. For the benefit of processing for research purposes, the Government proposes to consolidate provisions regarding research purposes and to define what is meant by "scientific research" in the UK GDPR and the Data Protection Act 2018 and also incorporate a clear definition of scientific research into legislation.

Removal of the legitimate interest balancing test

Many organisations rely on the legitimate interest legal basis to process personal data. However, there are various hurdles and assessments to be made as to the necessity of that processing and the balancing of those interests against the rights of data subjects. This can be an uncertain and complex process which the Government proposes to address by creating a limited list of legitimate interests for which organisations can use personal data without having to apply the balancing test.

AI and automated decision making

The Consultation recognises that data-driven AI systems could bring huge benefits, alongside a need to deploy AI tools that innovate responsibly and manage data-related risks at every stage of the AI life-cycle. The Consultation called for views on how the concept of fairness applies in the AI and machine learning field.

In particular, the Consultation invited evidence on proposals to remove or limit the restrictions on automated decision making (including profiling) under Article 22 of the GDPR. The current restrictions include the right to human review, giving individuals the right to challenge and request review

of a decision. The Government proposes the removal of this provision in its totality, instead permitting its use on the basis of legitimate interests or public interests.

Data minimisation and anonymisation

Current legislation provides that personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. This is commonly known as the 'data minimisation principle'.

At the moment, UK data protection legislation does not include a clear test for determining whether data is anonymous or not. In the interests of certainty, the Government has proposed to include a test for anonymisation in legislation, either by:

- placing Recital 26 of the UK GDPR onto the face of legislation, or
- creating a statutory test

The Government claims that greater use of effective anonymisation could help protect personal information, reduce risks for organisations and provide opportunity for broader economic and societal benefits.

Innovative data sharing solutions

The Government aims to encourage solutions that increase organisations' confidence and expertise in responsible data sharing practices. Therefore, the Government is considering its role in enabling activity of responsible 'data intermediaries' (e.g. entities that provide technical infrastructure and expertise to support interoperability between datasets or act as mediators negotiating sharing arrangements between parties looking to share, access or pool data).

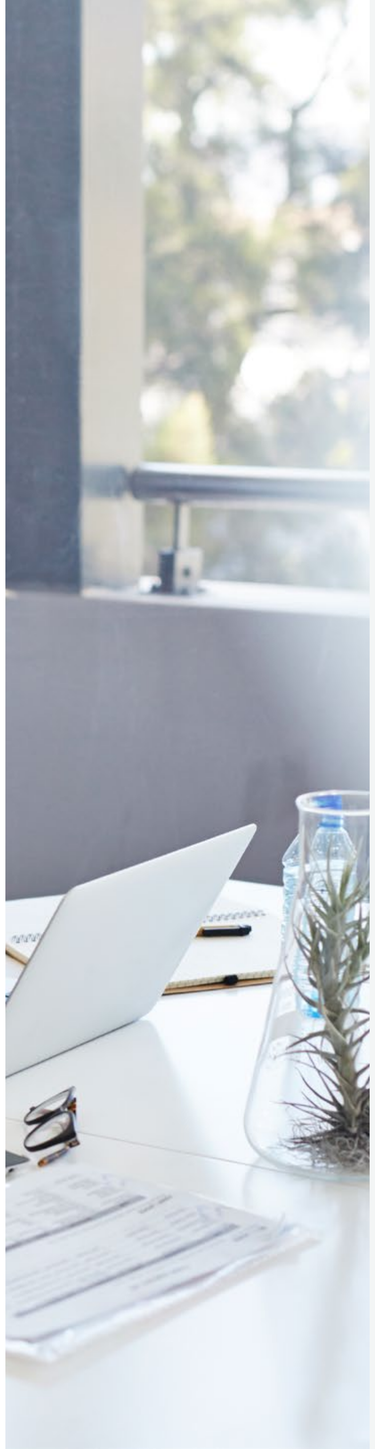
Chapter 2 – Reducing the burden on businesses and delivering better outcomes for people

Reform of the accountability framework

The accountability framework is comprised of the accountability principle in Article 5 of the UK GDPR. The accountability principle ensures effective data protection regulation and implementation and is also intended to support a number of outcomes, including: the protection of personal data; transparency; embedding data protection into organisational practices; enabling public trust; regulatory clarity and confidence in compliance; and facilitating enforcement activity.

The Consultation claims that, although the principle of accountability is fundamental, the current legislative framework sets out a number of specific requirements that organisations must satisfy in order to demonstrate compliance which creates a significant and disproportionate administrative burden on organisations. The changes being proposed by Government include the removal of the requirement to appoint a Data Protection Officer so that it can be replaced by a Privacy Programme manager, removal of the requirement to carry out a Data Protection Impact Assessment (**DPIA**) and removal of the requirement to consult with the ICO where high risk processing activities are being undertaken.

Significantly, the Government's proposals also seek to increase the threshold for reportable data breaches to the ICO to breaches where there is a '**material risk**' to individuals only.



Subject access requests

Subject access requests ('**SARs**') are a critical transparency mechanism and allow individuals to check the accuracy of their personal data, learn more about how their data is being used, with whom their data is being shared and obtain a copy of the data held about them. However, the Government has noted that these requests can cause difficulties for organisations in terms of their capacity to process these requests and the threshold for responding to a request.

Currently, Controllers can only refuse a SAR request or charge a reasonable fee if the request is either 'manifestly unfounded' or 'manifestly excessive'. However, the ICO has indicated that this provision is rarely utilised or relied upon.

To address these issues the Government is considering the introduction of a fee regime which will be similar to the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 ('**FOI**'). This fee regime would provide for payment of a fee for access to personal information held by all data controllers (the FOI fee limit is currently **£600** for Central Government and **£450** for public bodies).

Privacy and electronic communications

Whilst the focus of the Consultation remains firmly on reform of the UK GDPR, some elements of the proposals touch on the Privacy and Electronic Communications Regulations 2003 ("**PECR**"). The PECR complements the UK data protection framework but sets out more specific privacy rights for example, for electronic marketing.

As life has become increasingly digitised since the introduction of the PECR in 2003, the Government is considering the following:

- the removal of the requirement for consent for Analytics Cookies and other no risk trackers
- government invites comment on how to reduce consent fatigue for Cookie consent
- the expansion of a 'soft opt-in' to non-commercial organisations and the possible complete exemption of political parties from the PECR
- fine increases under PECR to match UK GDPR fines, and
- communication providers to be required to report fraudsters to the ICO

Chapter 3 - Boosting trade and reducing barriers to data flows

The Government has stated that it 'intends to facilitate digital trade and influence the global rules that govern the cross-border flow of goods, services and data.' This includes having the freedom to strike its own international data partnerships with global economies, using its data adequacy capability.

Adequacy

UK law allows the government to assess whether other countries' laws and practices provide an 'adequate' level of personal data protection. The Government has stated that it is committed to the reduction of barriers that organisations face when transferring personal data freely and safely overseas.

- To facilitate this, the Government has suggested the following:
- to ensure that all adequacy regulations made under current laws remain valid
- to approach adequacy assessments with a focus on 'risk-based' decision making in outcomes, and
- to relax the requirement to review adequacy regulations every four years

Alternative transfer mechanisms

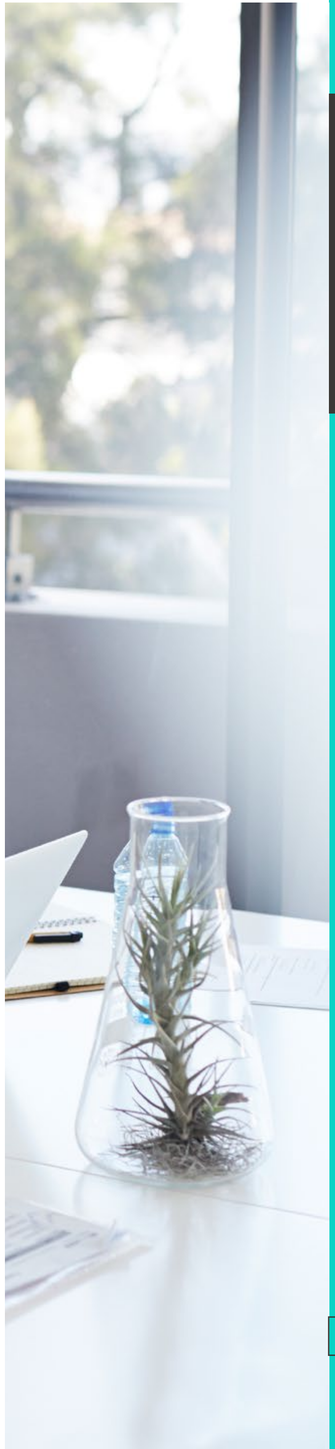
Alternative transfer mechanisms provide a route for cross-border transfers of personal data to countries that are not subject to an adequacy decision. Alternative transfer mechanisms are typically agreements which provide binding and enforceable protections for individuals' personal data when it is transferred internationally.

The Government is considering amendments to ensure the suite of alternative transfer mechanisms available to organisations in the UK GDPR are clear, flexible and provide necessary protections for personal data. The Government intends to introduce alternative transfer mechanisms and allow organisations to identify their own mechanism where appropriate.

Derogations

Derogations are outlined in Article 49 of the UK GDPR and are exceptions from the general rule that you should not make a restricted personal data transfer unless it is covered either by a UK adequacy regulation, or there are appropriate safeguards in place.

In the Consultation, the Government proposed to ensure that repetitive use of



derogations is permissible as repetitive use of derogations is currently restricted by UK GDPR. The Government claims this will provide flexibility and assurance for organisations that need to rely on derogations in certain limited but necessary situations.

Chapter 4 - Delivering better public services

The Government wishes to use personal data for the purpose of improving the delivery of public services while also maintaining a high level of public trust. Proposals in this regard support ease of data sharing – both between different public authorities, as well as between public bodies and private companies processing on their behalf. In particular, the Consultation clarifies that private companies, organisations and individuals who have been asked to carry out an activity on behalf of a public body may rely on that body's lawful ground of processing the data and do not have to identify a separate lawful ground to legitimise the processing of personal data.

Reform of the ICO

The Information Commissioner's Office (**ICO**) is the independent supervisory authority with responsibility for monitoring and enforcing the application of data protection legislation in the UK. The Government intends to improve the legislative framework that underpins the powers, role and status of the ICO, setting new and improved objectives and accountability mechanisms. This includes refocusing statutory commitments away from handling a high volume of low-level complaints and towards addressing the most serious threats to the public.

Additionally, the Government also proposes a new governance model for the ICO, aligning with the structure adopted by other regulators such as Ofcom and the FCA. This would remove the requirement for Parliamentary approval and allow The Secretary of State to appoint the CEO and approve (or reject) ICO guidance (with approval from HM Treasury).

Next Steps

The Consultation closed in November 2021 and the Government response is expected during 2022. If enacted, the proposals set out in the DCMS Consultation would significantly alter the UK's data protection framework and compliance requirements for businesses operating in the UK. The Government considers that the proposals would improve the current regime whilst maintaining the UK's "worldwide reputation for high data protection standards and security public trust".

There has already been much debate about the proposals with some arguing that the changes would dilute the rights of data subjects and weaken the data protections introduced by GDPR. However, there are no plans at present to revise the fines regime and that remains one of the biggest concerns for businesses when a maximum fine of £17.5m can be levied by the ICO. Will the proposed reforms jeopardise the adequacy finding granted to the UK by the European Commission? It is too early in the reform process to predict how the European Commission will react but it is a very real possibility. The extent to which the changes will radically alter the UK data protection landscape should become clearer in the coming year so watch this space.

A&L Goodbody

Key contacts

Mark Thompson
Partner
+44 28 9072 7591
mthompson@algoodbody.com

Aisling Byrne
Partner
+44 28 9072 7525
aibyrne@algoodbody.com

Ciaran O'Shiel
Partner
+44 28 9072 7448
coshiel@algoodbody.com

Resources

Data: a new direction — READ MORE

National Data Strategy — READ MORE