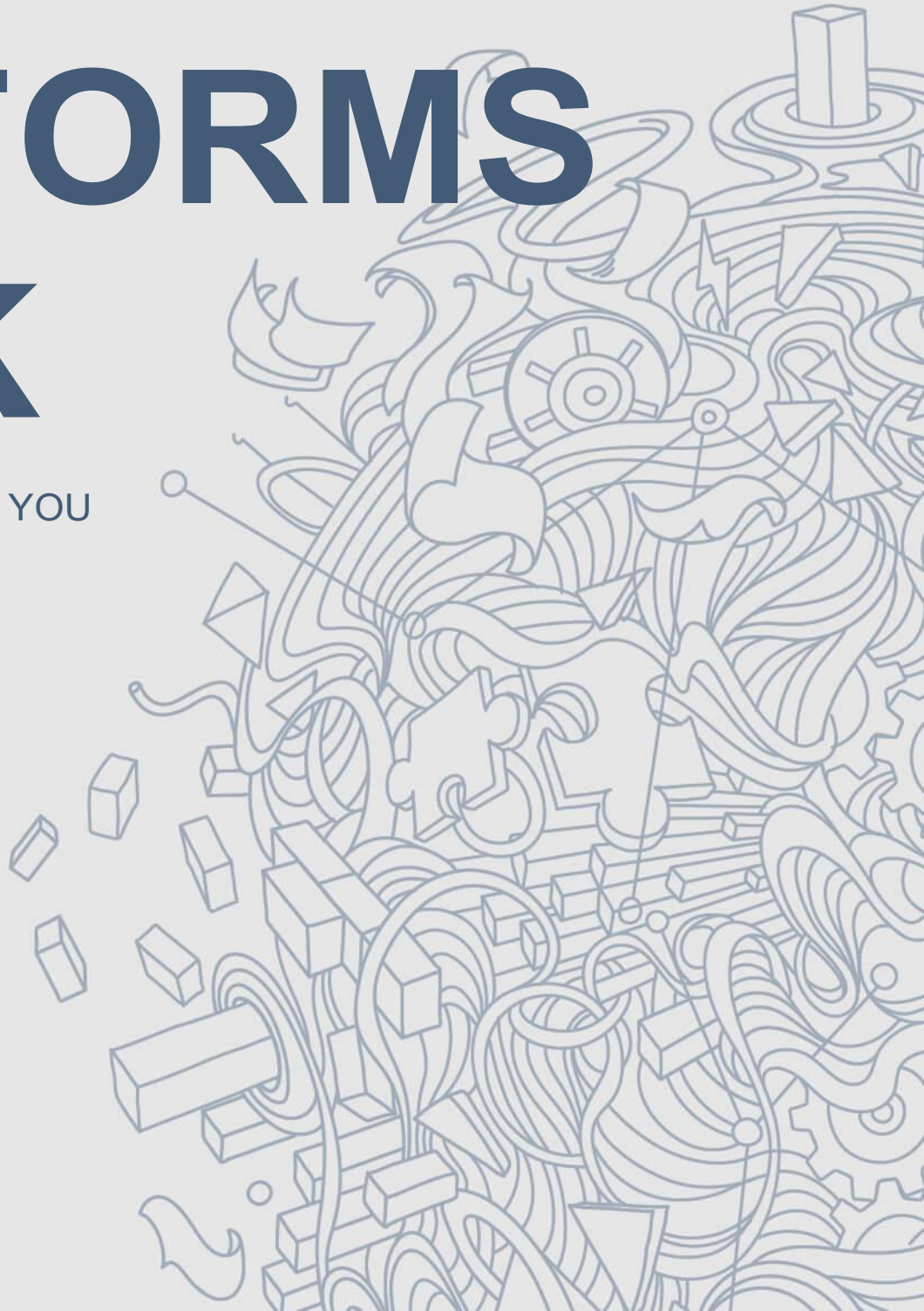
DATA REFORMS IN THE UK

SUMMARY OF CHANGES AND THEIR IMPACT FOR YOU



ADDLESHAW GODDARD

MORE IMAGINATION MORE IMPACT

DATA PROTECTION REFORMS IN THE UK – CHANGES AND HOW THEY MAY IMPACT YOU

On 17 June 2022 the DCMS published its long-awaited response to its Consultation, Data: a new direction.

Since the Consultation opened in September last year the UK government has received almost 3,000 responses, with huge issues at stake for UK businesses, citizens, trading partners, and the ICO.

It is the first significant indication of the direction that the UK's next data protection law will take, as the Government looks to reduce barriers to innovation and growth without undermining the UK's Adequacy Decision.

We have set out some of the key developments we can expect to see, and the potential impact of those changes for organisations processing personal data in the UK.

If you would like to discuss any of these changes, our Data Protection team are on hand to help you navigate these new challenges.

DATA REFORM IN THE UK – IMPACT OF CHANGES PROPOSED

CHAPTER 1: REDUCING BARRIERS TO RESPONSIBLE INNOVATION

Topic	Change Proposed	Potential Impact
Purposes of Processing	Creation of a definition of "scientific research" as a purpose for personal data processing.	Should improve clarity for researchers and provide more certainty about the additional purposes for which personal data can legitimately be used after it is collected. The government considers that this will facilitate innovation by removing barriers to progress (real or perceived).
Consent Changes	Clarifying the concept of "broad consent". This allows scientific research to rely on a less specific form of consent as a lawful basis, where it is not possible to fully identify the purpose of the processing when it is first collected.	This concept is already referenced in the recitals to the UK GDPR. However, expanding on this concept should provide greater certainty and scope for broader secondary use of personal data by researchers - without the need to provide additional information to data subjects about such use. This change means the government does not see the need to establish a new separate lawful basis for "research purposes".
Use of Legitimate Interests Assessments	Scaling back Legitimate Interest Assessments (**LIAs**). The government will produce a very limited list of processing activities for which the balancing test will not be required when conducting an LIA. For such activities, the government will assess whether additional safeguards needed regarding processing children's data.	This is a much more limited proposal than was first proposed, which suggested removing the balancing test from LIAs in general. The Response gives examples of activities which could appear on the initial list of crime prevention/safeguarding, or otherwise needed in substantial public interest. It will be interesting to see if this could be extended to cover some commercial activities at a later date.
AI Processing	Introduction of a new condition to Schedule 1 of the DPA 2018 to enable the processing sensitive personal data for the purpose of monitoring and correcting bias in AI systems.	In some instances, this is likely to provide a useful route to ensure that data processing to improve AI decision-making has a fair and lawful basis. However it is also potentially open to abuse, especially given the opacity of AI tools.
Anonymous Data	Clarifying where data is "anonymous", and when a living individual is identifiable and therefore within scope of data protection laws.	This could make it significantly easier to establish that data is not "personal" and is outside the scope of data protection law.

Topic	Change Proposed	Potential Impact
	The Response states that the test for identifiability is relative, and that the test should be based on the wording in the explanatory report to Convention 108:- *"Identifiable persons" means a person who can be easily identified: it does not cover identification of persons by means of very sophisticated methods*.	For example, data might only be personal where an individual is identifiable by the controller or processor by "reasonable means", or where the controller or processor knows, or ought reasonably to know, that passing the data to another data controller or processor is likely to result in re-identification. The final drafting of this clarification could have a very significant impact on the scope of the UK's new law.

CHAPTER 2: REDUCING BURDENS ON BUSINESSES AND DELIVERING BETTER OUTCOMES FOR PEOPLE

Topic	Change Proposed	Potential Impact
Privacy Management Programmes	There will be a new requirement for organisations to implement privacy management programmes (**PMPs**), replacing many of GDPRs accountability requirements.	This will allow many businesses to adopt a more flexible approach to data protection risk management, and bypass some of the measures that GDPR previously mandated. Whether these can genuinely offer an equivalent level of protection for individuals' data will depend on how the ICO chooses to police this obligation, and the guidance it publishes on what an effective PMP looks like for different types of business. The effectiveness of PMPs in safeguarding personal data will be a key factor in any potential challenge to the UK's Adequacy Decision from the European Commission.
DPO Requirement Removed	Removal of requirement to appoint a Data Protection Officer (**DPO**). Instead organisations will have to appoint a "senior responsible individual" to take responsibility for PMPs.	Many businesses will welcome this change. Article 38 GDPR imposes a number of onerous requirements around DPOs, including that they: • do not receive any instruction from management about the exercise of its tasks; • cannot be dismissed/penalised for emphasising data protection risks and refusing to bless high risk processing decisions; • have expert knowledge of data protection law; and • have access to the highest levels of management. It seems that other senior individuals with overall responsibility for PMPs will not be subject to these requirements, which may facilitate decision-making which is more tolerant of data protection risk.
Removal of Requirement to Run Data Protection Impact Assessments	Removal of requirement to conduct Data Protection Impact Assessments (**DPIAs**) where processing is "high risk". Organisations will still be required to ensure there are "risk assessment tools" in place for the identification, assessment and mitigation of data protection risks across the organisation.	The overall impact of this proposal is unlikely to become clear until the ICO begins enforcing the new law, and whether the difference between a DPIA and a Risk Management Tool is largely semantic. However, it is interesting that the test here will be whether risk management tools in are place, rather than ensuring that those tools are (a) fit for purpose;

Topic	Change Proposed	Potential Impact
		(b) actually used effectively; (c) used by people with sufficient data protection expertise to make those judgments. It certainly seems possible that data protection concerns might play a reduced role in decisions to roll out new technology and start processing personal data in new ways without a formal DPIA requirement.
Removal of Requirement to Maintain Records of Processing Activities	Removal of requirement to maintain records of processing (**ROPAs**).	Many organisations will welcome the option for greater flexibility to take a more tailored approach to record keeping. However, most organisations realise that effectively mapping data (including personal data) across the organisation is inherently valuable, and most are expected to continue with their existing practice. PMPs will still require effective data inventories.
ICO Engagement – High Risk Processing	Engaging with ICO before high-risk processing to become voluntary rather than mandatory. Where organisations choose to engage, this will be a mitigating factor in the event of a future breach.	Even where this was required, most organisations shied away from establishing a dialogue with the ICO to advertise their proposed high-risk data processing plans (for fear of being flagged as a company of concern and subject to subsequent monitoring/audit). This change seems to be a recognition of that reality, while maintaining an incentive for innovators who value data protection compliance highly to loop the regulator in to their future plans.
Changes to Data Subject Access Requests	Change to the current threshold for refusing a data subject access request (**DSAR**) or charging a reasonable fee for complying, from '*manifestly unfounded or excessive*' to '*vexatious or excessive*'.	A lot will hinge on the definition/interpretation of "vexatious" and how this is clarified in ICO guidance. However the ICO can expect a spike in complaints from data subjects whose access requests are dismissed as "vexatious". This seems like a question that would be tested through litigation sooner rather than later. The Response does not include a plan to introduce a fee for submitting a DSAR, which many had advocated for.

Topic	Change Proposed	Potential Impact
Cookie Consent	New rules on Cookie consent. The Response states that the government will remove the need for websites to display cookie banners to UK residents. In the immediate term, the government will permit cookies and trackers to be placed on user devices without obtaining explicit consent, for a small number of purposes deemed "non-intrusive" (i.e. website functionality and audience measurement, but not tracking). The government ultimately intends to move to a fully opt-out model of consent for all cookies (except those processing children's data), including tracking cookies, but will not do so until browser-based/similar solutions are widely available to help users to manage their preferences.	Cookies could be set without seeking consent from UK visitors, meaning publishers will be able to offer a more streamlined user experience without the need for a pop/up banner. However, the website must still give the user clear information about how to opt out, so background cookie policies on websites will still need to be kept up to date. Websites likely to have users which are children will need to continue using an opt-in consent model. It may be preferable for international organisations to maintain cookie banners/pop-ups where websites receive material traffic from the EU.

CHAPTER 3: BOOSTING TRADE AND REDUCING BARRIERS TO DATA FLOWS

Topic	Change Proposed	Potential Impact
Data Transfer Mechanisms	There will be a new power for the DCMS Secretary of State (**SoS**) to formally recognise new alternative data transfer mechanisms. The SoS will be able to create new UK mechanisms for transferring data overseas or recognise other international data transfer mechanisms, provided the SoS considers that they achieve the outcomes required by UK law.	The intention is that this reform will help to future-proof the UK's approach to international transfers and allow UK to be agile in responding to international developments. However, the European Commission will be particularly interested in any measures taken by the UK which could risk the protection of EU personal data transferred to the UK through an "onward transfer" to a country which the EU does not believe offers sufficient protection.
Adequacy for Data Transfers	When assessing the adequacy of the data protection laws of another country (for the purposes of allowing international data transfers without further protections), the recipient country may provide options for either administrative or judicial redress for UK data subjects, as long as the redress mechanism is effective.	While this may be an acknowledgement of the value of substance over form in the context of redress, it is another factor the European Commission may consider when gauging the risk attached to onward transfers of EU data.

CHAPTER 4: DELIVERING BETTER PUBLIC SERVICES

Topic	Change Proposed	Potential Impact
Use of Data by Public Authorities	Clarification of the lawful grounds for processing which are available to organisations when they are requested by a public body to help deliver outcomes in the public interest. Such organisations will be able to rely on the current basis under Article 6(1)(e) of the UK GDPR; i.e. you will not need to be a public sector body to rely on the condition that processing data is necessary for a public interest task, if you are *assisting* a public body with such a task.	In the past there has been a tendency to rely on legitimate interests when private sector organisations are asked to assist public bodies perform their obligations. However, recent events have highlighted the difficulties in relying on this approach. For example, legitimate interests cannot be relied on for the processing of special category data, such as health data. The new rules may make it easier for private/third sector organisations to assist with, for example, the government's response to a global pandemic.

CHAPTER 5: REFORM OF THE INFORMATION COMMISSIONER'S OFFICE

Topic	Change Proposed	Potential Impact
ICO Framework Changes	The government proposed introducing a new, statutory framework for the ICO which includes: • setting out the strategic objectives and duties that the ICO must aim to fulfil; • new statutory duties requiring the ICO to take greater account of competition, growth and innovation, and public safety in performing its function; • a new power for the DCMS SoS to prepare a statement of strategic priorities, which the ICO to have regard to when discharging its data protection functions; • moving away from the corporation sole structure and introducing a statutory board with a chair and chief executive; • a requirement for the ICO to carry out impact assessments to ensure the ICO's codes of practice and significant guidance are effective and useful, particularly for SMEs; and • introducing a process for the SoS to approve ICO codes of practice and statutory guidance before they are submitted to Parliament.	Individually, these changes may not have a dramatic effect on data controllers/processors and some may bring incidental benefits. For example, organisations may be able to gain greater insight into the ICO's priorities, make compelling arguments that risk of privacy harms could be justified by benefits in other domains (e.g. competition or innovation), and benefit from more targeted and business-friendly guidance. However, several consultation respondents (including the ICO itself) expressed concerns that these changes could undermine the ICO's independence and limit its ability to scrutinise the data processing practices of the public sector. This is likely to be highly relevant to the future assessment by the EU of the UK's Adequacy Decision.
New Complaint Model	Creation of a redress model that would require data subjects to seek resolution of their complaint directly with the data controller before lodging a complaint with the ICO. There would also be a requirement on data controllers to have a simple and transparent complaints-handling process in place.	Since Data Controllers are essentially already required to have simple and transparent processes to deal with data subject complaints, this is a pro-business change. It will create a barrier preventing data subjects from using a threat to go to the regulator until data controllers have had a sufficient opportunity to address the issue. Controllers with reasonably processes in place will gain a degree of protection from vexatious complaints.

CONTACT US

HELENA BROWN
Partner
+44 (0)7407 735118
+44 (0)131 222 9544

ROSS MCKENZIE
Partner
+44 (0)791 876 7330
+44 (0)1224 444328

DR NATHALIE MORENO
Partner
+44 (0)7921985931
+44 (0)20 7160 3179

CLAIRE EDWARDS
Partner
+44 (0)7795612964
+44 (0)161 934 6206

RICHARD CRAIG
Principal Knowledge Lawyer
+44 (0)7795002438
+44 (0)161 934 6759

MORE IMAGINATION **MORE IMPACT**

addleshawgoddard.com