CLIFFORD

CHANCE

THE UK'S DATA PROTECTION AND DIGITAL INFORMATION BILL – FURTHER REFORM ON THE HORIZON

THE UK'S DATA PROTECTION AND DIGITAL INFORMATION BILL – FURTHER REFORM ON THE HORIZON

The UK's **Data Protection and Digital Information Bill** (**Bill**) was laid before the UK Parliament on 18 July 2022, marking a significant step in the post-Brexit reform of the UK's data protection regime. The Bill, which followed the Department for Digital, Culture, Media and Sport's (**DCMS**) **"Data: A New Direction" consultation** earlier this year, proposed amendments to various pieces of UK legislation, including the UK's incorporation of the EU's General Data Protection Regulation into domestic law (**UK GDPR**), the Data Protection Act 2018 (**DPA**) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (**PECR**).

The Bill forms a crucial part of the UK's **National Data Strategy**, which aims to demonstrate post-Brexit opportunities for "unlocking the value of data" and "securing a pro-growth and trusted data regime", while seeking to retain the UK's adequacy status under the EU's General Data Protection Regulation (**EU GDPR**) and Law Enforcement Directive, preserve strong data subject rights and allow multinational businesses to navigate diverging regulatory regimes. Although much of the Bill builds on the UK's existing data protection framework (which is based on the EU GDPR), it nevertheless proposes some significant changes that would impact not only UK entities but also entities elsewhere that are caught by the territorial scope of the laws amended by the Bill.

The Bill's passage through the UK's legislative process was paused in September 2022 to allow for further consideration following changes to the UK's governmental leadership. The Bill is expected to re-enter the legislative process in due course, preceded by a short period of time for DCMS to engage with businesses and civil society in relation to possible amendments. Many businesses and other stakeholders are, therefore, currently considering the Bill with this engagement window in mind.

This briefing analyses key aspects of the Bill and highlights areas that are likely to be the focus of engagement on potential further reform. To assist the reader in understanding the amendments to other pieces of UK data protection legislation, we have also produced **Keeling Schedules** (redlines) of the UK GDPR, DPA and PECR.

CORE THEMES OF THE BILL

Facilitating data processing

- Revised definition of "personal data"
- Use of automated decision-making
- Purpose limitation and further processing
- Lawfulness of processing
- International transfers of personal data
- Use of personal data for scientific research purposes
- Cookies and other changes to PECR

New provisions for data access and Digital Verification Services

- Introduction of Digital Verification Services
- Introduction of Smart Data Regime

Reduction in administrative burden

- Data subject rights
- Data Protection Officer / Senior responsible individual and appointed representatives
- Records of processing
- Assessment of high-risk processing / Data Protection Impact Assessments

Enforcement and regulatory oversight

- Information Commission and its role
- Complaints by data subjects
- Enforcement

THEME 1: FACILITATING DATA PROCESSING

If enacted in its current form, the Bill would facilitate certain types of data processing by redefining the parameters of what constitutes "personal data", removing certain requirements and prohibitions, applying exemptions, and creating greater legal certainty regarding the permissibility of certain forms of personal data processing. Below we examine key examples of such provisions.

Change to the definition of "personal data"

Key changes

The UK GDPR and DPA regulate the processing of personal data relating to an identified or identifiable natural person. The Bill seeks to clarify, and arguably somewhat narrow, the circumstances in which an individual may be considered "identifiable". Specifically, under the Bill, an individual would only be considered "identifiable" if:

- they are identifiable by the controller or processor by reasonable means (being those that the person is reasonably likely to use) at the time of the processing; or
- where the controller or processor knows, or ought reasonably to know that:
  - another person will, or is likely to, obtain the information as result of the processing; and
  - the individual will be, or is likely to be, identifiable by that person by reasonable means (being those that the person is reasonably likely to use) at the time of the processing.

Analysis

If the Bill proceeds in its current form, these provisions would:

1. Clarify that the assessment of identifiability would only take into account means of identification which are available to the controller, the processor or others who will, or are actually likely to, receive the data – disregarding third parties who might have the means to identify the data subject but are unlikely ever to access the data. This would settle an often debated point of legal interpretation;
2. Clarify that identifiability should be assessed at the time of processing – e.g., clarify that where an organisation receives personal data without identifiers, but with a right to gain access to the identifiers on the occurrence of defined events in the future, such data is not personal data until such events occur; and
3. Introduce a test of the likelihood of identification of an individual from the data by a controller, processor or third party under which only means which are *reasonably likely to be used* by that person to identify an individual would be taken into account (provided an individual is not immediately identifiable from the data). This would apparently exclude means that the relevant person *could* use (it would be technically feasible to do so) but is *unlikely to use in practice*. Notably:
   - While the Bill includes a list of factors to be taken into account in this assessment (such as time, cost, effort and resources), due to the non-exhaustive nature of this list the assessment of whether a person is likely to identify an individual from the data using reasonable means could, if interpreted broadly, arguably include other factors restricting such identification – such as legal or contractual restrictions or even internal policies or technical and organisational measures.
   - This interpretation could mean that data relating to living individuals which are separated from relevant identifiers fall outside the scope of UK data protection laws in a wider range of circumstances than is currently the case – perhaps including where the same organisation holds the relevant identifiers in a separate repository with no intention of applying these in order to identify individuals.

If the text remains unchanged, organisations could, in theory, benefit from opportunities for data analytics, innovation and data sharing created by the narrowed definition – particularly organisations adopting broad interpretations of these provisions. In practice, however, for many organisations managing data under multiple data protection regimes, trying to take advantage of such changes on a large scale would likely be hindered by difficulties in separating data that is subject only to UK data protection laws from other

data (that is subject to, for example, the EU GDPR). It would also involve costly and potentially impracticable adjustments to existing processes and documentation. Consequently, many multinational organisations may continue to deploy data protection controls on the basis of the existing definition of personal data in many circumstances.

The Bill's next iteration

The next version of the Bill may include greater clarity in relation to these provisions, thereby reducing the likelihood of: (i) organisations adopting significantly diverging approaches; or (ii) subsequent regulatory guidance narrowing the interpretation of these provisions in a manner that may diverge from the government's intention when drafting the Bill. However, such clarity could have the unwelcome consequences of either: (i) limiting the impact of these changes through solidifying a narrow interpretation; or (ii) creating a greater risk to the EU's adequacy decision for the UK by highlighting the degree of change introduced to the definition of personal data.

Use of Automated Decision-making

Key changes

- The Bill seeks to narrow the existing restrictions on the legal bases that can be relied upon when making decisions with a legal or similarly significant effect based solely on automated decision-making (**ADM**). Under the Bill, these restrictions would now only apply where special category personal data is used.
- Existing safeguards (such as transparency and contestability requirements) apply to all significant decisions made using personal data and based solely on ADM – including those falling outside the newly narrowed restrictions on legal bases for processing.
- The Bill provides that the Secretary of State may, by regulation, specify certain decisions as having the required significant effect for the data subject (thereby triggering the safeguards) and add to, vary or make specific requirements in relation to the safeguards.

Analysis

A key benefit of these changes would be that ADM could be used for significant decisions even where the legal basis for processing is legitimate interest – a legal basis widely relied upon for a range of business operations – without the need to insert meaningful human involvement into the decision-making process. For businesses that are able to separate data that are subject only to UK privacy laws from data that are subject to the EU GDPR, this change could greatly facilitate use of ADM through artificial intelligence and machine learning technologies.

The Bill's next iteration

The scope of what constitutes a 'significant decision' remains uncertain pending regulation by the Secretary of State or regulatory guidance on the point, particularly in relation to the use of profiling. The Explanatory Notes to the Bill might be expanded to greater effect in this regard.

Given the other legislative reform currently underway in the UK which is likely to impact explicability, transparency and accountability for algorithmic processing, fair treatment and duties to consumers and related liability regimes, alignment across these legislative proposals will be important to ensuring the emergence of a coherent framework.

DCMS may also find itself requested by industry to consider adding an ability for the Secretary of State to authorise certain uses of ADM involving special category data, in order to future-proof these provisions.

Purpose limitation and further processing

Key changes

The Bill restates the purpose limitation principle to state that personal data shall be collected (whether from the data subject or otherwise) for specified, explicit and legitimate purposes and not be further processed by or on behalf of a controller in a manner that is incompatible with the purposes for which the controller collected the data.

The Bill also brings together various existing provisions relating to the compatibility of further processing purposes and adds an annex of additional processing purposes which can safely be considered compatible with the original purpose(s) for which the data was collected (and therefore permitted). At present, these lists of purposes focus on processing for reasons of public interest, public security, emergency response, crime prevention and detection, safeguarding, taxation and compliance with law. The Secretary of State may make regulations that would vary or add to the list of compatible processing.

Analysis

Purpose limitation principle: Depending on how "the controller" is interpreted in the restated purpose limitation principle, this could mean that controllers need only consider the compatibility of further data processing by reference to the purposes for which they themselves collected the data (and not by reference to the purposes for which the data may have originally been collected from the data subject by another controller).

Compatible further processing purposes: Several of the compatible processing purposes listed in the annex are broadly framed and may therefore prove helpful in enabling organisations to confidently undertake certain further processing. For example, the inclusion in this list of processing for the purposes of detecting, investigating or preventing crime may facilitate certain compliance-related processes.

The Bill's next iteration

Further clarity would be beneficial in relation to how the restated purpose limitation principle should be applied to the reuse of datasets in controller-to-controller data sharing scenarios. Similarly, although our reading of the compatible processing purposes listed in the newly inserted provisions of the UK GDPR is that these are non-exhaustive, the next version of the Bill might use the Explanatory Notes to expressly clarify that the provisions do not operate to exclude other compatible purposes.

It is possible that the next iteration of the Bill would also see an expansion of the list of compatible further processing purposes, streamlining compatibility decisions in relation to personal data processing that is subject only to UK laws. Alternatively, if the Bill becomes law in its current form, the role of this list in streamlining compatibility decisions may instead evolve in significance over time through secondary legislation.

Lawfulness of Processing

Key changes

The Bill proposes to introduce a new lawful basis for processing, namely processing that is necessary for the purpose of "recognised legitimate interests". The "recognised legitimate interests" – listed in a new annex to the UK GDPR – are automatically deemed to have a legitimate interest lawful basis without requiring an assessment balancing such interest with the rights and interests of the relevant data subject(s).

At present, these lists of purposes focus on processing for reasons of public interest, public security, emergency response, crime prevention and detection, safeguarding, and democratic engagement. As with the list of compatible further processing purposes, the Secretary of State will have the ability to amend or vary "recognised legitimate interests" grounds.

Analysis

As with the provisions relating to compatible further processing, several of the recognised legitimate interests are, helpfully, broadly framed and may therefore prove helpful in enabling organisations to confidently undertake certain further processing. Businesses should note, however, that they would not be permitted to rely on these recognised legitimate interests for ADM that results in a significant decision. In these cases, a legitimate interest balancing assessment would still be required. This may limit the practical benefit of this change in a number of circumstances.

The Bill's next iteration

Given the current focus of EU courts on the use of the legitimate interest legal basis, DCMS may decide to continue with the current list of recognised legitimate interests in the next iteration of the Bill, rather than seeking to expand it. Instead, the role of this list in streamlining certain data processing decisions may expand over time if it is expanded through secondary legislation.

International Transfers of Personal Data

Key changes

Under the Bill, transfers of personal data to a third country or an international organisation are permitted if they are:

- approved by regulations made by the Secretary of State (i.e., the UK's equivalent to EU adequacy decisions), which involves the Secretary of State completing a data protection test and fulfilling certain ongoing monitoring obligations;

- made subject to appropriate safeguards (which mirror the existing safeguards in Article 46 of the UK GDPR) and the transfer meets the standard of a data protection test; or
- made in reliance on a derogation (with these being largely unchanged from the existing regime).

The data protection test to be applied by data exporters making transfers using appropriate safeguards would operate in a manner similar to transfer risk assessments introduced through *Schrems II* and subsequent regulatory guidance. However, the standard of protection proposed is a protection that might not be *materially lower* than the standard in the UK (which may be considered to differ from the "essential equivalence" standard referred to in EDPB guidance on risk assessments for international transfers of personal data).

Notably, when making regulations to approve transfers, the Secretary of State may have regard to any matter which he or she considers relevant, including the desirability of facilitating transfers of personal data to and from the UK.

The Secretary of State may make a number of changes to the international transfer-related provisions through regulations, including providing for other appropriate safeguards.

Analysis
It is debatable whether there is a significant gap between "materially lower" and "essentially equivalent" when assessing the data protection standards of a third country for the purposes of a personal data transfer, and it is unclear how the Secretary of State's ability to take into account the desirability of facilitating transfers would interact with the assessment made to approve transfers through regulations. Therefore, the impact of such changes on international data transfers under the UK GDPR and DPA remains unclear and the potential effect on the EU's adequacy decision for the UK even more so, given that it will also likely be heavily influenced by political factors. Even if the text as it currently stands may not jeopardise EU adequacy, the interpretation, use and any further modifications to these provisions (if enacted) will, no doubt, be closely monitored by the EU. In particular, any approved free flow of data from the UK to jurisdictions that are currently in the EU spotlight could well endanger the UK's adequacy decision.

The Bill's next iteration
In this part of the Bill the tensions between seeking to facilitate international trade, on the one hand, and maintaining the UK's EU adequacy decision, on the other hand, are perhaps most visible. Discussions between UK government officials and European counterparts will be crucial in order to ensure the right balance is struck in relation to these particularly sensitive provisions.

Use of personal data for scientific research purposes

Key changes
The Bill sets out how references within the UK GDPR to processing for certain types of research and statistical purposes should be interpreted. Notably this includes adding that scientific research will mean "*any research that can reasonably be described as scientific*".

The Bill makes a number of amendments which benefit data processing falling within the definition of scientific research purposes. In particular, subject to certain safeguards:

- it allows a general consent to processing for an area of scientific research where it is not possible to fully identify the scientific purposes (subject to certain conditions); and
- in relation to processing for research, archiving and statistical purposes, the Bill expands the "impossibility or disproportionate effort" exemption to the requirement to provide a privacy notice for further data processing such that it also applies to data collected directly from a data subject (with the ability to consider factors such as the number of data subjects, age of the personal data and appropriate safeguards in determining what would involve a disproportionate effort).

Analysis
While some of these amendments largely import guidance from the recitals of the UK GDPR, and the additional language does not in itself clarify the scope of "scientific research", the changes nevertheless indicate that a broad interpretation of "scientific research" is encouraged.

The Bill's next iteration
Businesses may seek more clarity as to the extent to which certain types of commercial research and development activities can be considered to fall within the scope of this definition and therefore benefit from some of the changes made to facilitate data processing for scientific research purposes. However, it is perhaps more likely that this would be addressed through subsequent regulatory guidance rather than clarifications to the Bill itself, given the balance to be struck with maintaining the UK's adequacy decision from the EU.

Cookies and other changes to PECR

Key changes
Cookie consent requirements: The Bill seeks to widen the situations where cookies and similar tracking technologies ("cookies") can be used without the end-user's consent. The exceptions to consent, where an opt-out could instead be relied upon, are expanded beyond "strictly necessary" cookies to include (subject to certain conditions) the use of cookies to:

- make improvements to a service, website or app;
- allow the appearance or functions of a website or app to adapt to the preferences of the subscriber or user, or otherwise enable an enhancement of the appearance or functionality of the website or app when displayed on, or accessed by, the device; and
- make software updates for security of the user's device.

Alternative mechanisms for managing cookie preferences: The Bill empowers the Secretary of State to make regulations that would require providers of certain (as yet unspecified) technologies to give users the ability to express their cookie consent preferences via alternative preference management systems (such as browser-based and device-based opt-outs).

Duty to notify: The Bill introduces new regulations which place a duty on public electronic communication service and public communication network providers who have reasonable grounds for suspecting that a breach of the PECR might be occurring to report it to the renamed Information Commission within 28 days of first becoming aware of such activity. This provision is very broadly drafted and it is unclear how organisations would be expected to comply in practice, although the absence of a positive obligation to investigate or monitor compliance may influence interpretation of this duty by regulators.

Enforcement: The Bill updates the PECR enforcement regime to bring it in line with that of the UK GDPR and the DPA. Notably, this increases potential fines to GPDR levels.

Analysis
While the intention of these changes is to facilitate the lower-risk use of cookies and improve user experience in relation to cookie consent, this may not be achieved in practice if the Bill is enacted in its current form. Businesses subject only to the UK cookie requirements are likely to welcome being able to rely on an opt-out model (rather than consent) for a range of lower-risk uses of cookies and similar technologies, although it remains to be seen how broadly these purposes will be interpreted (in particular in relation to enhancements of websites, and app appearance and functionality). However, businesses that are subject to cookie requirements under other laws may still decide to collect consent for some of these activities given the complexity of effectively deploying different consent collection strategies according to the relevant applicable laws. The practical impact of this reform is also further limited by the industry shift towards use of first-party data rather than third-party cookies.

The push to address the issue of centralised management of cookie consents (and move away from repeated presentation of cookie consent pop-ups) is also likely to be broadly welcomed. However, the drafting of the Bill indicates that it is not yet clear how this might be achieved in practice. Leaving aside issues regarding whether technological solutions yet exist that can implement this effectively while preserving privacy rights, it is unclear how this model would operate on a multi-jurisdictional basis if EU authorities require a different approach to the collection of cookie consents. Adding to the complexities in this area will include: (i) competition concerns regarding standard setting for the centralised cookie management service; and (ii) questions surrounding the allocation of responsibility and liability for the effective operation of third party-managed cookie preference management models.

The Bill's next iteration

Given the technical and legal complexities involved, these provisions may be an area of focus for DCMS in any further industry engagement undertaken on the draft proposals, in order to give them the best chance of working effectively. In this consideration window, the DCMS may also consider how to assist UK businesses to appropriately utilise first party data (particularly in the context of the Smart Data Regime we discuss below), given the industry shift away from third-party cookies.

THEME 2: FACILITATING DATA PROCESSING

Other changes proposed by the Bill are likely to be less significant than those addressed above, with a focus on incremental reductions in the administrative burden of compliance with privacy laws. However, it should be noted that, for organisations that will also have to comply with the EU GDPR and other privacy laws, these changes may not result in any simplification of privacy-related governance processes. In a few (thankfully limited) cases, these changes may in fact create additional complexity for multinational businesses due to their divergence from the EU GDPR. Below are key examples of aspects of the Bill aimed at reducing administrative processes relating to data protection.

Data Subject Rights

Key changes

The Bill would amend the "manifestly unfounded or excessive" exemption for refusing to respond to (or charging a fee for responding to) the exercise of data subject rights under the UK GDPR. This is replaced with an exemption where requests are "vexatious or excessive", which potentially expands the circumstances in which such requests may be refused. The Bill provides a non-exhaustive list of factors to be considered when determining whether a request meets this new threshold, including whether the request is intended to cause distress or are not made in good faith, and requests that are an abuse of process.

In addition, a new provision is included which clarifies when a controller can 'stop the clock' in calculating the applicable time period for responding to the exercise of a data subject's right (which largely restates existing regulatory guidance).

Analysis

It remains to be seen how the test(s) of "vexatious or excessive" would be applied in practice. For example, it is unclear whether "excessive" will be considered a substantially lower threshold than "manifestly excessive" (the interpretation to the provision used by the ICO in **guidance**), and whether having a single list of factors to consider in relation to the threshold for rejecting a data subject's request (in relation to both "vexatious" and "excessive") might preclude reliance on (helpful) existing regulatory guidance in relation to the meaning of "manifestly excessive". The term "vexatious" is used in section 14 of the Freedom of Information Act 2000 and whilst there is some case law and **regulatory guidance**, it remains a largely untested provision and much will hinge on the ICO's interpretation and further guidance. This change might, for example, serve to lower the threshold for applying the exemption and help address the risk of "weaponising" the use of data subject access requests.

The Bill's next iteration

Businesses will be keen to understand whether the inclusion of "abuse of process" as a form of vexatious request will allow for refusal to act on data subject access requests that seek to circumvent a court or tribunal disclosure process.

Data Protection Officer (DPO) replaced with Senior Responsible Individual (SRI) and removal of requirement to appoint representatives

Key changes

The UK GDPR currently requires the designation of a data protection officer (DPO) where processing is carried out by a public authority, or where an organisation's core activities consist of: (i) systematic monitoring of data subjects on a large scale; or (ii) large-scale processing of special category or crime-related data. Under the Bill, this would be replaced with a requirement to designate a senior individual (or individuals) who would be responsible for data protection matters where processing is carried out by a public authority, or where an organisation carries out high-risk processing. The senior responsible individual(s) would need to be part of the organisation's senior management. The Bill provides different tasks for senior responsible individuals depending on whether their organisation acts as a controller or processor in relation to the relevant data processing.

The Bill would also remove the requirement for organisations outside the UK that are caught by the UK GDPR to appoint UK-based representatives.

Analysis
If the Bill proceeds in its current form:

- Organisations whose current DPO is not a member of senior management would need to identify a suitable member of senior management to take on the SRI role, and consider what training that person would require in order to fulfil the duties of the SRI;
- Organisations that previously took the view that they were not required to appoint a DPO will need to consider whether the appointment of an SRI is required;
- External DPO appointments may need to be reviewed;
- Companies that appointed a group DPO may also need to review these arrangements: it is unclear whether appointment of a single SRI across multiple legal entities in a corporate group would be permitted under the current drafting, as the requirement for an SRI to be part of an organisation's senior management could be interpreted to apply to each legal entity; and
- Companies that are subject to the Financial Conduct Authority's Senior Manager and Certification Regimes will also be seeking clarity as to whether and how those rules would apply in relation to the SRI.

The Bill's next iteration
Many organisations are hoping to see significant changes to these provisions in the next version of the Bill, perhaps querying why the current DPO requirement is being amended.

Records of Processing

Key changes
The Bill would require that organisations maintain "adequate" records of the processing of personal data. It largely simplifies the information that controllers and processors must log in these records (previously termed "record of processing activities" or "ROPAs"); for example, by removing the obligation for the controller to detail all categories of data subjects and personal data (reserving this for special category and crime-related personal data only) and by removing the obligation for processors to maintain records of processing delineated according to the applicable controller.

Certain provisions might, however, be read as being more prescriptive than the current requirements. For example, the Bill would introduce a requirement for controllers and processors to identify where personal data is (whether it is in the UK or abroad) which appears to differ from the current requirement to identify transfers of personal data to a third country or international organisation.

Analysis
If the Bill were enacted in its current form, the completion and maintenance of records of processing would, generally, be simplified for organisations that are subject only to the UK GDPR or that are able to separate their processes to benefit from these simplifications. For businesses that are also subject to the EU GDPR, maintaining existing records would meet the majority of the proposed new UK GDPR requirements, subject to limited exceptions (for example, regarding the location where data is recorded).

The Bill's next iteration
The next iteration of the Bill might make amendments so that organisations retain the option to maintain their current records of processing.

Assessment of High-risk Processing (previously Data Protection Impact Assessments, or "DPIAs")

Key changes

The Bill would replace the obligation to conduct a data protection impact assessment (**DPIA**) with an "assessment of high-risk processing" (**Assessment**). The Bill would remove the list of circumstances in which an organisation is required to conduct a DPIA (instead relying on the requirement that the Information Commission (the proposed replacement UK data protection supervisory authority) will publish a list of the kind of processing that requires an Assessment) and simplifies aspects of the Assessment process. Notably, the Bill would make consulting the Information Commission optional where an Assessment indicates processing would result in high-risk processing (where this was previously mandatory).

Analysis

For businesses subject only to the UK GDPR, if these proposed changes become law, they may ease privacy-related compliance burdens through less prescriptive risk assessment processes and removal of mandatory consultation requirements (which were rarely triggered in practice). Businesses that are also subject to the EU GDPR would likely be able to maintain their DPIA process while still meeting the new UK GDPR requirements, subject to monitoring the list of circumstances in which these assessments are required under the UK GDPR (once published).

The Bill's next iteration

The Bill's next iteration may see few, if any, changes to these provisions.

THEME 3: NEW PROVISIONS FOR DATA ACCESS AND DIGITAL VERIFICATION SERVICES

The Bill proposes introducing entirely new data governance regimes which: (i) provide a framework for digital verification services; and (ii) pave the way for regulations impacting data access and governance beyond personal data – including requirements for "data holders" to make available "customer data" and "business data" to customers or third parties.

Digital Verification Services

Key changes

Building on the existing framework set out in the **UK digital identity and attributes trust framework – beta version**, the Bill proposes the introduction of a new regime for Digital Verification Services (**DVS**). The new regime would consist of four primary components:

1. **a trust framework:** The Secretary of State would, in conjunction with consultations with the Information Commission, prepare and publish a trust framework (i.e., rules and standards for the provision of DVS).
2. **a register:** The Secretary of State would establish and maintain a DVS register, listing bodies that provide DVS services and making it publicly available. To be listed on the register, DVS bodies would need to satisfy certain criteria, including holding a certificate issued by an accredited conformity assessment body.
3. **an information gateway:** The information gateway would allow public authorities to disclose information to a registered DVS provider for the purpose of digital verification.
4. **adoption of a trust mark:** The Secretary of State would have the power to designate a trust mark to be used only by those organisations on the DVS register.

Analysis

Businesses that currently have a need to verify the identity of customers and users may be considering the extent to which use of DVS could improve their ability to do so. If the Bill proceeds in its current form, these provisions may pave the way for requirements regarding the use of DVS in certain circumstances, such as those addressed in the Online Safety Bill, which may override existing uses of proprietary DVS systems. Significant impacts of this may be felt where there are currently no positive obligations to verify due to a lack of identity infrastructure and may, for example, affect how businesses approach age verification.

The Bill's next iteration

One option available to DCMS would be to separate these provisions into a stand-alone legislative proposal.

Smart Data Regime

Key changes

Building on the ***Smart Data Working Group's policy paper*** (published in Spring 2021), the Bill acts to establish a Smart Data regime for the UK. To do this, the Bill would confer powers on the Secretary of State and Treasury to make regulations that:

- would require data holders to provide customer data and business data either directly to an individual at their request or to a person authorised by the individual to receive the data; and
- requires data holders to:
  - respond to requests to provide or publish customer data or business data to an individual or to an authorised recipient;
  - to produce, collect or retain customer data;
  - implement changes to customer data, including the rectification of inaccurate customer data;

- use specified facilities or services, including dashboard services, other electronic communication services or application programming interfaces (APIs); and
- create complaint-handling and dispute resolution procedures.

The scope of the data that would be subject to the Smart Data Regime is broadly defined in the Bill:

- **Consumer Data** covers information relating to a customer of a trader including information relating to transactions between the customer and the trader.
- **Business Data** relates to:
  - information about goods, services and digital content supplied or provided by the trader;
  - information relating to the supply or provision of goods, services and digital content by the trader (such as, for example, information about where they are supplied, the terms on which they are supplied or provided, prices or performance); and
  - information relating to feedback from customers about goods, services or digital content.

The enforcement of this Smart Data Regime includes investigatory powers, as well as the power to impose financial penalties.

Analysis
Given the breadth of the definitions and the reliance on secondary legislation, the scope of the Smart Data Regime may be far-reaching if it becomes law in its current form. For instance, it might allow the Government to require data holders to make "customer data" and "business data" available to not only customers but also to third parties, which could include competitors.

If the Bill proceeds in its current form, there will remain a significant degree of uncertainty regarding how this new regime will operate. For example, it is unclear from the Bill whether the roll-out or implementation of the smart data regime is intended to be UK-wide or to have a sectoral focus, or how this regime would operate in relation to regulated sectors. It is also currently not clear whether the regulations would provide protection for confidentiality or other restrictions on processing.

The Bill's next iteration
Given the significance of these proposals and their potential implications for the way many businesses invest in, and compete on the basis of, data collection and generation, these provisions may be an area of focus for DCMS in any further industry engagement undertaken on the draft proposals, in order to ensure they work effectively.

THEME 4: ENFORCEMENT AND REGULATORY OVERSIGHT

The Bill seeks to make wide-ranging changes to the UK's data protection supervisory authority, replacing the Information Commissioner (and the associated Information Commissioner's Office) with the Information Commission. This includes granting the Secretary of State greater influence and oversight in relation to the Information Commission's activities. It also includes provisions which would allow the Information Commission to deploy its powers more strategically.

Information Commission and its role

Key changes

The Information Commissioner will be replaced with an Information Commission, a body more closely resembling other statutory regulators such as Ofcom and the CMA. Under the Bill, in carrying out its duties the Information Commission must have regard to, amongst other things, the desirability of promoting innovation and competition – with the Information Commission even being required to consult on how the manner in which it exercises its functions may affect economic growth, innovation and competition when preparing a strategy for carrying out its functions. The Bill would empower the Secretary of State to designate a Statement of Strategic Priorities from time to time which sets out Government's strategic priorities relating to data protection, and require the Information Commission to have regard to this in exercising its functions. The Bill would also impose reporting requirements for the Information Commission against the Statement of Strategic Priorities and certain performance indicators.

Analysis

A statutory basis for a data protection supervisory authority to have regard to innovation would be novel, with potential benefits for the UK economy.

The possibility of increased power and influence by the Government in the operation of the Information Commission would no doubt be closely monitored by the EU authorities if the Bill were enacted in its current form, noting that the independence of a data protection supervisory authority is a consideration in adequacy decisions.

The Bill's next iteration

Consultation with civil society and discussions between UK government officials and European counterparts will be important in order to understand, and perhaps address, potential concerns regarding the independence of the Information Commission.

Complaints by Data Subjects

Key changes

The Bill would give the Information Commission the right to refuse to act on certain complaints received from data subjects, where:

- the complaint has not been made to the controller; or
- the complaint has been made to the controller but a 45-day period for the controller to handle the complaint is ongoing; or
- the complaint is vexatious or excessive.

Analysis

These changes would likely reduce the number of complaints that the Information Commission receives and make it easier for problems to be resolved between a controller and data subject before they are escalated to the Information Commission.

The Bill's next iteration

The Bill's next iteration may see few, if any, changes to these provisions.

Enforcement

Key changes

The Bill would grant the Information Commission power to require the preparation of a report (at the controller's or processor's expense) when exercising its investigatory powers. Where the Information Commission suspects that a controller or processor is breaching data protection law, it would be able to issue an interview notice, requiring a manager or member of staff to attend an interview to answer questions. Giving a false statement in response to an interview question would be an offence.

Analysis

If the Bill is enacted, companies would need to be prepared to respond to assessment notices and interview notices. In practice, this would mean:

- ensuring that data protection accountability documentation is in place and maintained;
- conducting regular data protection training for all staff members who have data protection responsibilities; and
- fostering strong working relationships with key relevant suppliers involved in personal data processing.

The Bill's next iteration

The Bill's next iteration may see few, if any, changes to these provisions.

NEXT STEPS

The Bill seeks to balance the Government's ambitions of promoting responsible innovation and easing compliance burdens, on the one hand, with the desire to preserve strong individual data rights, maintain the UK's EU adequacy decision and allow multinational businesses to navigate diverging regulatory regimes, on the other.

Key priorities for businesses in relation to the Government's consideration of the Bill are likely to be ensuring that refining the UK's data protection regime does not: (i) entail the rebuilding of data protection programmes – which would require significant investment by business and disruption to operations; (ii) create additional complexities in navigating multijurisdictional data governance programmes through incompatibilities with, for example, EU rules; or (iii) come at the cost of limiting the free flow of personal data between the EU and the UK by jeopardising the EU's adequacy decision.

In order to thread this needle, it will be crucial that the Government uses this pause in the Bill's legislative process to consult with industry and civil society, align the Bill with other proposals for UK legislative reform, and enter into discussions with European counterparts and stakeholders to ensure risks and concerns are identified and resolved.

AUTHORS

Simon Persoff
Partner
T: +44 20 7006 3060
E: simon.persoff@cliffordchance.com

Rita Flakoll
Global Head of Tech Group Knowledge
T: +44 20 7006 1826
E: rita.flakoll@cliffordchance.com

Richard Jones
Director of Data Privacy
T: +44 20 7006 8238
E: richard.jones@cliffordchance.com

Lauren Murphy
Associate
T: +44 20 7006 2228
E: lauren.murphy@cliffordchance.com

James Wong
Associate
T: +44 20 7006 3750
E: james.wong@cliffordchance.com

Ioana Burtea
Associate
T: +44 20 7006 1699
E: ioana.burtea@cliffordchance.com

CONTACTS

Jonathan Kewley
Partner, Co-head of Global Tech Group
T: +44 20 7006 3629
E: jonathan.kewley@cliffordchance.com

Kate Scott
Partner
T: +44 20 7006 4442
E: kate.scott@cliffordchance.com

Samantha Ward
Partner
T: +44 20 7006 8546
E: samantha.ward cliffordchance.com

Nelson Jung
Partner
T: +44 20 7006 6675
E: nelson.jung@cliffordchance.com

Phillip Souta
Head of UK Public Policy
T: +44 20 7006 1097
E: phillip.souta@cliffordchance.com

Aniko Adam
Counsel
T: +44 207006 2201
E: aniko.adam@cliffordchance.com

Sally Murphy
Senior Associate
T: +44 20 7006 4574
E: sally.murphy@cliffordchance.com

Arnav Joshi
Senior Associate
T: +44 20 7006 1303
E: arnav.joshi@cliffordchance.com

Oscar Tang
Senior Associate
T: +44 20 7006 3749
E: oscar.tang@cliffordchance.com

Laia Bertran Manye
Senior Associate
T: +44 20 7006 8919
E: laia.bertranmanye@cliffordchance.com

Haafiz Suleman
Senior Associate
T: +44 20 7006 4348
E: haafiz.suleman@cliffordchance.com

Mark Comber
Senior Associate
T: +44 20 7006 2398
E: mark.comber@cliffordchance.com

Jamie Andrew
Senior Associate
T: +44 20 7006 1367
E: jamie.andrew@cliffordchance.com

Herbert Swaniker
Senior Associate
T: +44 20 7006 6215
E: herbert.swaniker@cliffordchance.com

Midori Takenaka
Senior Associate
T: +44 20 7006 1593
E: midori.takenaka@cliffordchance.com

Claudia Hall
Lawyer
T: +44 20 7006 2523
E: claudia.hall@cliffordchance.com

Fadeia Hossian
Knowledge Lawyer
T: +44 20 7006 6238
E: fadeia.hossian@cliffordchance.com

Hemin Hazar
Lawyer
T: +44 20 7006 3828
E: hemin.hazar@cliffordchance.com

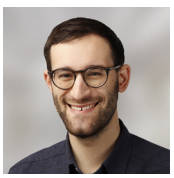
Nicole Kidney
Lawyer
T: +44 20 7006 1302
E: nicole.kidney@cliffordchance.com

Alex Dixey
Lawyer
T: +44 20 7006 3323
E: alex.dixey@cliffordchance.com

Adam Hunter
Lawyer
T: +44 20 7006 1499
E: adam.hunter@cliffordchance.com

Linda Agaby
Lawyer
T: +44 20 7006 3125
E: linda.agaby@cliffordchance.com

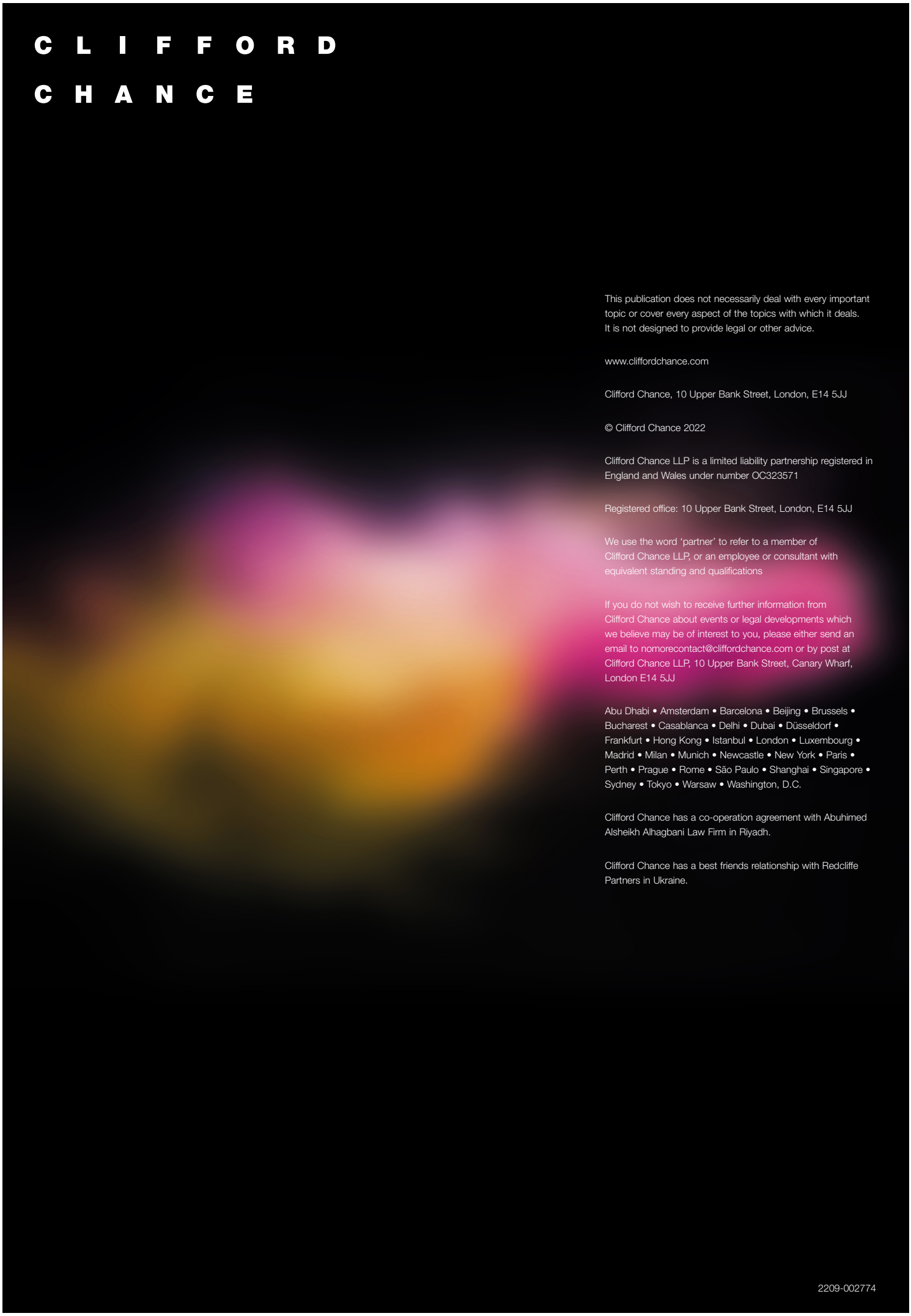
William Hanway
Lawyer
T: +44 20 7006 6190
E: william.hanway@cliffordchance.com



Eliot Cohen
Lawyer
T: +44 20 7006 2966
E: eliot.cohen@cliffordchance.com

CLIFFORD

CHANCE



This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

© Clifford Chance 2022

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

2209-002774