19 November 2021

Comments by the Centre for Information Policy Leadership on the UK Department for Digital, Culture, Media and Sport's Consultation on Reforms to the Data Protection Regime

The Centre for Information Policy Leadership (CIPL)[1] welcomes this opportunity to provide comments to the UK Department of Digital, Culture, Media and Sport (DCMS) on its consultation on reforms to the UK's data protection regime.[2] CIPL supports the UK government's ambition to secure an improved data protection regime that supports a world-leading digital economy across the UK. CIPL has previously provided input to DCMS' consultation on the UK National Data Strategy[3] and welcomes this opportunity to provide further input into specific proposals to enhance UK data protection requirements.

CIPL appreciates DCMS' efforts in thinking so carefully and thoroughly about all the different areas presented in the consultation. In particular, DCMS has identified several important issues to be addressed to enable a modern digital economy that effectively protects privacy while enabling the responsible and beneficial use of personal data, and has put forward several robust solutions to many of the key challenges.

In this submission, CIPL provides input into many of the proposed reforms, focusing specifically on the following chapters:

- Chapter 1: Reducing Barriers to Responsible Innovation;
- Chapter 2: Reducing Burdens on Businesses and Delivering Better Outcomes for People;
- Chapter 3: Boosting Trade and Reducing Barriers to Data Flows; and
- Chapter 5: Reform of the Information Commissioner's Office

This submission also considers the views gathered from CIPL members during two roundtables that CIPL organized with DCMS on 13 and 14 October 2021 to obtain feedback on the reform proposals. A collation of the viewpoints put forward at the roundtable is attached as an appendix to this submission. The appendix was previously submitted to DCMS**.** Many of the issues addressed in the appendix are in addition to the ones addressed in the present consultation response.

---

[1] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] Data: A New Direction, UK Department for Culture, Media & Sport, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf.

[3] CIPL's response to the UK National Data Strategy Consultation, 2 December 2020, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_uk_national_data_strategy_consultation__2_dec_2020_.pdf.

By way of general observations, we would note that the scope and scale of the consultation is far-reaching as well as detailed – an extensive and ambitious undertaking. The length and breadth of the consultation will generate long and detailed responses. Many of these responses will be caveated, as respondents, such as CIPL, welcome certain proposed reforms, but also raise concerns about perceived or potential dilution of safeguards which may have an adverse or negative impact on the UK data protection framework and world-leading approach to data. We would therefore encourage DCMS to not only review each of the responses from the many responding organisations within each theme/section, but also to consider what the impact would be of the proposed reforms as a whole and having considered the feedback obtained.

By way of comparison, one of the challenges of the UK Data Protection Act 2018, is that while it includes many important clarifying provisions which supplement the UK GDPR, it is very challenging to read and understand, and results in significant complexity, which ultimately leads to confusion and a lack of accessibility of the requirements to all but the most sophisticated reader. We would encourage DCMS to consider the UK data protection legislation as a whole, in terms of its provisions, its outcomes and its accessibility to those to whom it applies (government, business SMEs, individuals, academia, etc.). A coherent, accessible and understandable articulation of the objectives of the legislation should be driving the reform agenda, thereby achieving a balanced outcome. The concern is that tweaking and tinkering may lead to more complexity and less clarity, and the result may be seen as a less robust version of the EU GDPR rather than as a distinctive UK approach to data protection which promotes high data protection standards in a clear framework, supporting innovation and digitalization, and encouraging inward investment to the UK.

Another reality to be taken into consideration is that the eyes of the world are on the UK as it carves a new path and future in data and digitization. Being ambitious and forward thinking is what will be expected and welcomed as the outcome of this data reform review, but there will also be considerable scrutiny as to whether the UK's approach will amount to a lowering or dilution of data protection standards. This will be of particular concern to those jurisdictions with whom the UK has agreed adequacy arrangements, especially the EU, which continues to be one of the UK's largest trading partners globally. It would be unhelpful to all aspects of the UK economy and society if the UK's approach were to be seen as reckless or negatively impacting data protection in its outcome. As businesses well know, reputations take time and effort to build, but can be lost far more quickly, and in many cases, cannot be rebuilt. As businesses make decisions about where to locate their leadership and operations, their decisions are driven by multiple factors including the credibility of the data regime from which they are operating, and it is this credibility on the world stage that we would advocate as being the backbone of the reforms being considered.

At CIPL, we are encouraged by the proposed approach to further embrace the Accountability Principle, which is at the core of the UK GDPR but could be strengthened, and the support for Privacy Management Programmes – a clear sign post to organisations to move from tick box compliance to a culture of compliance and accountability, where privacy is integrated into organisational operations and strategy. This approach encourages organisations to apply data protection requirements to their specific organisational structures and business models, enabling privacy to be integrated into technology, security, risk, compliance, legal, business and other functions as a practical reality rather than a separate, siloed step, which is often perceived as a barrier and hurdle to be overcome. Such Privacy Management Programs would not replace existing accountability mechanisms but would integrate them as elements of

a holistic approach to accountability and compliance via a comprehensive organisational Privacy Management Program. We also support expanding the ability of organisations to rely on the "legitimate interest" basis of processing, as well as an overall strengthening of the related risk-based approach to data protection, which enables calibration of legal requirements and safeguards based on the level of risk associated with data processing. However, with this organizational risk-based accountability structure, there is a balance to be achieved with respect to all aspects of the reform proposal to ensure that individual rights are also safeguarded and can be readily exercised when needed. And it is this critical balance that the outcome of the UK Data Protection Reform will be judged on.

We therefore support and encourage DCMS in its continued efforts to set out a definitive UK, world-leading approach to data protection, which supports innovative uses of data while ensuring high data protection standards. We also urge DCMS to apply a "common sense" approach to how the data protection regime is articulated, applied, enforced and continues to develop, including with the aims of attracting foreign investment and encouraging international engagement and interoperability on data protection, particularly for data transfers. Finally, we would caution against framing the ICO-related proposals in terms of "reforming" the ICO. The ICO is a highly effective and globally respected data protection authority. We would instead characterise any amendments to the ICO's powers and responsibilities as further strengthening the ICO and expanding upon its current capabilities.

We hope that you find our submission useful as DCMS continues to work on improving the UK data protection regime and if you would like to discuss any of our comments or require additional information, please contact Bojana Bellamy, bbellamy@huntonak.com.

Chapter 1: Reducing Barriers to Responsible Innovation

A. Scientific Research

1. *Proposal: Consolidating and bringing together research-specific provisions and incorporating a clearer definition of "scientific research" into legislation.*

CIPL agrees that relevant provisions related to processing for research purposes are dispersed across existing legislation and welcomes the proposal to consolidate these provisions together into a clear definition. CIPL also believes that any new research definition should be framed flexibly as research is dynamic by nature and increasingly relies on the use of AI.

By including a clear yet flexible definition, the UK will:

- Enable beneficial research, including by commercial entities, for the public interest and societal advancement;

- Provide much needed clarity to organisations that struggle with determining whether to pursue specific research projects in light of data protection concerns (e.g., through clarifying that research includes a broad range of activities, including for Research and Development purposes);

- Facilitate exploratory research without a stated hypothesis as often times the point of AI-based research is to generate new hypotheses that might never surface without engaging in such exploration;

- Encourage organisations to be innovative in supporting national and global initiatives to support ESG goals and outcomes;

- Empower organisations in appropriately balancing the rights of individuals with research objectives and pursuing research efforts in a balanced way.

2. *Proposal: Creating a new, separate lawful ground for research, subject to suitable safeguards and clarifying in legislation how university research projects can rely on tasks in the public interest as a lawful ground for personal data processing.*

CIPL supports the creation of a separate lawful ground for research as this would promote certainty and consistency for organisations. However, CIPL highlights that departing too much from the approach under the GDPR could add complexity to the processing activities of multinational organisations that would have to navigate different legal regimes for cross-border research efforts. In that regard, the updated UK data protection regime may acknowledge that conformity with the original standard under the UK GDPR for research efforts would be acceptable for compliance purposes in cases of cross-border research projects. Moreover, CIPL recommends clarifying what types of safeguards would be suitable in order to rely on a new research processing ground, i.e., an articulation of "what good looks like". This clarity should be provided by way of regulatory guidance rather than in the law itself.

With respect to the proposal to clarify in legislation how university research projects can rely on performance of a task in the public interest as a legal basis for research, CIPL would like to highlight that such an approach would exclude certain researchers from engaging in beneficial research (e.g., self-funded or industry-driven research) that may well be in the public interest. Private entities should be considered as contributing to the public interest when public and private organisations are working collaboratively on research projects. Moreover, research must be looked at through a broad lens, with privately funded and commercial research and development viewed as equally important to public interest research and enabled in law. Indeed, given the pressures of funding for universities, there is an increasing trend for universities to look to the private sector for funding, particularly for innovative research projects.

CIPL believes that the optimal approach would be to enable certain research projects, both university research projects and others, through reliance on the lawful ground of performance of a task in the public interest and to include a separate ground for research processing, subject to suitable safeguards, in a revised regime. This provides maximum flexibility for organisations to engage in research efforts while still ensuring the safeguarding of the rights of individuals.

Separately, CIPL wishes to bring to DCMS' attention the lack of legal clarity on the interplay between Article 6 and 9 of the GDPR when special category data (i.e., health data) is processed, and whether both articles apply cumulatively or can be assessed separately (which is the preferred approach). It is often difficult for the industry to determine the correct legal basis for use in the research context as scientific

research only relates to Article 9 but not to Article 6. DCMS has an opportunity to provide clarity on this issue through its reform efforts.

3. *Proposal: Clarifying in legislation that data subjects should be allowed to give their consent to broader areas of scientific research when it is not possible to fully identify the purpose of processing at the time of collection.*

CIPL agrees that it would be beneficial to clarify in law that broad consent can be given by data subjects for future research purposes. Often, the potential relevance and usefulness of data for specific purposes only becomes apparent after it has been collected (e.g., mobility data collected in the weeks preceding the start of the COVID-19 pandemic proved invaluable in assisting public health officials to effectively coordinate appropriate responses and social distancing measures in certain geographic regions, a use of collected data which could not have been foreseen prior to the pandemic outbreak). Of course, consent cannot be so broad as to enable any use of data for any purpose that may arise in the future. CIPL believes that an approach enabling broad consent for research purposes is sufficiently curtailed to ensure that the data is only used for future beneficial purposes in the public and societal interest.

B. **Further Processing**

1. *Proposal: Clarifying that further processing for an incompatible purpose may be permitted when it safeguards an important public interest.*

CIPL agrees that the compatibility test of Article 6(4) of the GDPR should be refined to clarify that processing for incompatible purposes may be permitted when such processing safeguards an important public interest. The COVID-19 pandemic serves as a good case study for such processing, whereby there was an important public interest in processing the location data of individuals to coordinate appropriate health responses and contact tracing efforts in the initial stages of the pandemic. While a global pandemic is perhaps an obvious example, there are many business examples which may also apply, such as data collected in the customer relationship context which may be used and analysed to support developing ESG obligations.

2. *Proposal: Clarifying the circumstances in which further processing can be undertaken by a controller different from the original controller, while ensuring fairness and transparency.*

Given the increasing digitilisation of every aspect of our lives both in the workplace and as a society, and the essential reality of data sharing and transfers (whether to leverage emerging areas of expertise or to benefit from innovative data processing), both in the public and private sectors, CIPL believes that clarifying the circumstances in which further processing can take place by a controller different to the original controller, would be useful for organisations. CIPL cautions, however, that such rules should be framed flexibly and broadly and subject to further regulatory guidance given that the data sharing landscape is still developing and many new data sharing legal regimes are currently under development globally. If DCMS crafts a law that only enables sharing data for further processing under specific circumstances this may unnecessarily limit the ability of new controllers to receive and process such data. Moreover, any rules that are directly applicable to the new controller with respect to further processing should also be appropriately framed to ensure that data subject rights are safeguarded and to promote the beneficial outcomes of uses of data.

C. **Legitimate Interests**

1. *Proposal: Creating a limited, exhaustive list of legitimate interests for which organisations can use personal data without applying the balancing test in order to give them more confidence to process personal data without unnecessary recourse to consent.*

CIPL appreciates that DCMS recognizes that overreliance on consent for processing in the modern digital environment can present significant practical and legal challenges, and that it has been a strong proponent of alternative lawful grounds to consent which provide more relevant and appropriate grounds for processing, including legitimate interests. This is particularly important for all those firms that provide services, infrastructure and expertise within a given sector, but have limited or no direct relationship or contact with the individual to which the data relates. Given the pace and innovation of data processing, the multiple parties involved, and the increasing complexity and sheer volume of data processing, it is even more critical to identify appropriate and flexible bases for processing other than informed consent which may be neither relevant or appropriate, and is increasingly generating consent fatigue for individuals. DCMS correctly notes that one reason organisations continue to rely on consent for many processing operations is because they find the UK GDPR to be unclear with respect to alternative legal processing grounds and when they may be appropriately used.

While CIPL believes that consent has an important role to play in circumstances where it can be effective (i.e., where individuals can be effectively informed about their choices and are able to make a choice), it would be very useful for any update to the UK data protection regime to provide more clarity on when the legitimate interest ground may be relied upon by organisations. In fact, providing more legal certainty with respect to using the legitimate interest ground and thereby encouraging its use when it is appropriate, is one of the most important elements of the UK's reform proposal. CIPL has previously categorized and produced examples and case studies of legitimate interest processing (e.g., for fraud detection and prevention, employment data processing, product development and enhancement and processing "data for good") and these categories may be instructive in providing further clarity on legitimate interests as a legal basis in addition to the DCMS's own list contained in the consultation report. A list of categories of common processing activities based on legitimate interests can be found in CIPL's July 2021 White Paper on "How the 'Legitimate Interests' Ground for Processing Enables Responsible Data Use and Innovation".[4]

CIPL also strongly supports creating a whitelist of low risk "legitimate interest" processing activities. However, it should be made clear that including a processing activity on such a whitelist only removes the burden of conducting the balancing of potential interests, rights and freedoms of individuals against the legitimate interest of the organization or a third party; it does not absolve organisations from complying with other UK GDPR requirements, including purpose limitation, adequacy of the data, privacy by design, proportionality, fairness, as well as implementing appropriate risk-based safeguards.

[4] CIPL White Paper "How the 'Legitimate Interests' Ground for Processing Enables Responsible Data Use and Innovation", July 2021, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_how_the_legitimate_interests_ground_for_processing_enables_responsible_data_use_and_innovation__1_july_2021_.pdf.

Further, while the UK data protection law should enable such a legitimate interest whitelist and might also provide broad parameters for processing activities that should be included, CIPL recommends that the law assign the creation of a this whitelist to the ICO. Thus, the ICO would consider the processing activities set forth in the consultation report and others for inclusion in this list. By delegating such a task to the ICO, there is an opportunity to update and revise the list and any appropriate accompanying guidance as technologies and business practices evolve, rather than trying to make a change in the law after it has been passed.

a. *B2B data and professional contact information*

An example of a low-risk activity that that should be included in a "legitimate interest" white list by the ICO is B2B data and the processing of basic professional contact information. The processing of B2B data presents far lower risks to the rights and freedoms of individuals than the processing of B2C data. This is particularly true for B2B direct marketing and processing basic professional contact information. In relation to direct marketing, the Information Commissioner's Office ("ICO") itself notes that "*the expectations of individuals about how personal data is used in their business capacity are likely to be different to their expectations about how data is used in their personal capacity*. *For example, an individual whose business contact details are publicly available on their employer's website may well expect to receive contact from other businesses*."[5] In its guidance on legitimate interests, the ICO also seems to accept that processing B2B data is lower risk than processing B2C data. One question the ICO asks in its legitimate interests balancing test criteria is the question "*Is it data about people in their personal or professional capacity*?"[6], suggesting that processing personal data about an individual's professional capacity is less intrusive. Thus, the processing of B2B data, and particularly the subset of business contact information, presents limited risks to the rights and freedoms of the individual because the data is:

a. not sensitive, insofar as it does not reveal any special category or criminal data about an individual;

b. rarely private, and is often publicly available or available after reasonable inquiries;

c. unlikely to relate to a child.

Given the context of processing business contact information, it is also extremely unlikely that an individual could experience an adverse effect or any distress from standard processing operations, and in any event any such impact on the data subject could be mitigated by the data subject's exercise of their Article 21 UK GDPR right to object.

CIPL agrees with the consultation's note that there is significant uncertainty about when it is possible to rely on the lawful ground of legitimate interests under Article 6(1)(f) UK GDPR and that this uncertainty must be remedied. This is true in particular for B2B communications and marketing. Despite clear regulatory signals that the processing of B2B data is likely to be lower risk (as set out above), there continues to be uncertainty for businesses to enable them to make this assessment with confidence in the absence of the allocation of significant time and resource to assess each case, and the assumption of

[5] https://ico.org.uk/for-organisations/direct-marketing/business-to-business-marketing/.
[6] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/.

possible regulatory risk. This contrasts in particular with other jurisdictions, where processing business contact information is subject to a more pragmatic regulatory approach, proportionate to potential harm, or is excluded from the scope of data protection laws altogether:

- In Singapore, business contact information (unless it is provided only for personal purposes) is largely exempt from the provisions of the Personal Data Protection Act ("**PDPA**").

- In Canada, the Personal Information Protection and Electronic Documents Act ("**PIPEDA**") excludes business contact information such as an employee's name, title, business address, telephone number or email addresses when it is collected, used or disclosed solely for the purpose of communicating with that person in relation to their employment or profession. This Canadian approach acknowledges that processing such B2B data is inherently lower risk to the rights and freedoms of individuals.

- In Canada, there are also limited restrictions on the use of B2B data for email marketing as section 6 of Canada's anti-spam legislation does not apply to B2B commercial electronic messages sent by an employee, representative, consultant, or franchisee of an organisation to another employee, representative, consultant, or franchisee of the organisation if the organisations have a relationship, and if the message concerns the activities of the organisation to which the message is sent.

In sum, CIPL proposes to reform the UK data protection framework to allow the ICO to establish a list of low risk processing activities that meet the "legitimate interest" ground for processing, and that this list include processing business contact information for the purpose of initiating and maintaining a commercial relationship (including sales, recruitment and marketing purposes). Not only would this approach not undermine the rights of individuals under the UK GDPR, who would still have the right to object under Article 21 as well as benefit from other relevant GDPR protections, it would align the UK with other international approaches and would improve legal certainty for organisations with respect to the legitimate interest processing ground. Currently, organisations often feel compelled to take an approach to legitimate interests that is overly conservative and may overestimate the risk of an incorrect legitimate interests balancing test, thereby skewing the balance against both themselves and the data subject, depriving data subjects from the benefits of processing. Moreover, businesses thrive on the ability to communicate with each other about prospects and to collaborate and action these opportunities. Finally, by clarifying that B2B communications for the purpose of initiating and maintaining a commercial relationship can rely on legitimate interest without a balancing test, the UK would also enable resource and budgets to be allocated in a more beneficial way. Of course, a similar analysis applies to the other types of processing that would be included in such a whitelist.

D. <u>AI and Machine Learning</u>

1. *Fairness*

DCMS has not put forward a specific proposal for addressing the concept of fairness in an updated UK data protection regime. CIPL appreciates that DCMS acknowledges that there is uncertainty surrounding the scope and substance of fairness in data protection as applied to the development and deployment of AI systems. Fairness can have different and not always compatible meanings depending on differing circumstances/contexts, and in the evolving context of AI, it would be premature to specify what this

means. CIPL also welcomes DCMS' consideration that horizontal or sectoral laws and regulators may provide a more appropriate avenue for the assessment of some aspects of fairness, and also that this issue may be dealt with in future under the UK's AI governance framework.

To the extent that any updated UK data protection regime seeks to elaborate on the concept of fairness, CIPL believes that the proportionality test outlined in Canada's proposed Consumer Privacy Protection Act[7] (CPPA) can be instructive, as fairness can be seen as linked to proportionality, although this is not necessarily the only approach that should be considered. Section 12(1) of the CPPA notes that an organisation may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances. Factors to consider in determining whether purposes are appropriate include: (a) the sensitivity of the personal information; (b) whether the purposes represent legitimate business needs of the organisation; (c) the effectiveness of the collection, use or disclosure in meeting the organisation's legitimate business needs; (d) whether there are less intrusive means of achieving those purposes at a comparable cost and with comparable benefits; and (e) whether the individual's loss of privacy is proportionate to the benefits in light of any measures, technical or otherwise, implemented by the organisation to mitigate the impacts of the loss of privacy on the individual.

2. *Proposal: Stipulate that processing personal data for purposes of ensuring bias monitoring, detection and correction in relation to AI systems constitutes a legitimate interest for which the balancing test is not required.*

CIPL agrees that DCMS should clarify that processing personal data to prevent, detect and remediate bias in AI systems constitutes a legitimate interest of the data controller. However, in line with CIPL's comments above, this type of processing should not absolve an organization from the responsibility of assessing and mitigating risks of the processing in its specific context.

3. *Proposal: Create a new condition within Schedule 1 of the Data Protection Act 2018 which specifically addresses the processing of sensitive personal data as necessary for bias monitoring, detection and correction in relation to AI systems.*

CIPL supports DCMS' proposal to create a new condition within Schedule 1 of the Data Protection Act 2018 to address processing sensitive data to prevent, detect and remediate bias in AI systems.

CIPL believes that DCMS' alternative proposal does not sufficiently address the objective of bias monitoring, detection or correction, i.e., the proposal of making clear that processing of sensitive data can fall under the existing derogation in paragraph 8 of Schedule 1 of the Data Protection Act of 2018 relating to processing of sensitive personal data for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment of specific vulnerable people. This provision would limit processing for bias monitoring to vulnerable populations and thus would not be appropriate or realistic for broader bias monitoring beyond just vulnerable populations.

[7] An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts, available at https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading.

Organisations are increasingly required and encouraged to be proactive in ensuring diverse, equal and inclusive workplaces. In order to support organisational objectives to be transparent and to identify and address areas where they are falling short of their objectives to be diverse, equal and inclusive employers, they need to be able to consider the full range of protected characteristics together with areas such as social background inclusion, in order to be employers of choice. CIPL encourages amendment of this provision to enable organisations to achieve this valid social and business objective in the processing of sensitive and other categories of data.

4. *Automated Decision-Making Rules*

As with the concept of fairness, DCMS is not proposing specific changes to the right not to be subject to automated decision-making under the UK GDPR. However, DCMS acknowledges that it is important to examine whether Article 22 and its provisions are keeping pace with the likely evolution of a data-driven economy and society, and whether it provides necessary protection. CIPL wishes to highlight the following points for consideration by DCMS:

- Right to be invoked vs direct prohibition: CIPL's view is that the right not to be subject to solely automated decision-making that produces legal or similarly significant effects is a right to be invoked by data subjects rather than a direct prohibition on such automated decision-making in the absence of an exception.[8] The more restrictive direct prohibition interpretation which has been put forward by the EDPB prevents any such decisions from being conducted under the legitimate interest ground for processing. CIPL has stressed that under this interpretation, it is critical that the meaning of a legal and similarly significant effect be interpreted narrowly to ensure that beneficial automated decision-making is not inadvertently banned unless one of the three narrow exceptions apply. The UK is not obliged to follow this same interpretation and there is scope for the UK to rethink the approach to Article 22. Of course, DCMS may consider that deviating from the GDPR approach at this stage might not be optimal, especially for multinational companies which engage in automated decision-making on a global scale. It may make more sense for DCMS to focus its reform on clarifying the current approach and, in particular, the meaning of a legal or similarly significant effect (see comments below). Nevertheless, CIPL believes that both options should be carefully considered by the UK before it settles on a final approach.

- Meaning of legal effect and similarly significant effect: Globally, Article 22 has created a trend of uncertainty among organisations, as well as data privacy regulators, which are still exploring what constitutes an impactful automated decision for purposes of Article 22. For example, the UK ICO has noted that that it is very difficult to compile a list of examples that would be thorough enough to be informative. They suggest an alternative way to think about such impacts—by asking relevant questions in a specific context. The ICO noted that certain factors may assist in this determination, such as the psychological effects of the decision and whether an individual knows that his or her behavior is being monitored. The Office of the Australian Information

[8] CIPL comments on the Article 29 Working Party's Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, December 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_wp29_data_portability_guidelines_15_february_2017.pdf.

Commissioner (OAIC) has commented that the notion of a "similarly significant effect" under Article 22 is quite vague and believes that it should apply in the context of "bigger" decisions. The OAIC believes that some of the current draft privacy legislation in the United States could provide additional clarification in this context. For example, some draft laws propose a non-exhaustive list of "significant effects" which include denial of consequential services or support, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities and health care services.[9] CIPL believes that DCMS has an opportunity to clarify this issue for organisations that are struggling to understand their Article 22 obligations. By being proactive on this issue, the UK could lead the way forward for other jurisdictions that are increasingly introducing data protection rules around automated decision-making. CIPL has previously shared with the UK government a list of automated decisions that it considers produce legal effects and similarly significant effects and those that it does not believe produce such effects. We reiterate these again below for DCMS to consider as it thinks further about any specific changes to automated decision-making under an updated UK data protection regime.

Decisions Producing Legal Effects	• Decisions affecting the legal status of individuals • Decisions affecting accrued legal entitlements of a person • Decisions affecting legal rights of individuals • Decisions affecting public rights—e.g., liberty, citizenship, social security • Decisions affecting an individual's contractual rights • Decisions affecting a person's private rights of ownership
Decisions Producing Similarly Significant Effects *Some of these examples may also fall within the category of legal effects depending on the applicable legal regime and the specific decision in question.*	• Decisions affecting an individual's eligibility and access to essential services—e.g., health, education, banking, insurance • Decisions affecting a person's admission to a country, their citizenship, residence or immigration status • Decisions affecting school and university admissions • Decisions based on educational or other test scoring–e.g., university admissions, employment aptitudes • Decisions to categorise an individual in a certain tax bracket or apply tax deductions • Decisions to promote or pay a bonus to an individual • Decisions affecting an individual's access to energy services and determination of tariffs

[9] See Privacy Act Review–Issues Paper, Submission by the Office of the Australian Information Commissioner, December 2020, available at https://www.oaic.gov.au/assets/engage-with-us/submissions/Privacy-Act-Review-Issues-Paper-submission.pdf at page 95. The laws cited include the Consumer Rights to Personal Data Processing Bill SF 2912 (Minnesota); New York Privacy Bill SB 5642 (New York); and the Protecting Consumer Data Bill SB 5376–2019-20 (Washington State).

Decisions <u>Not</u> Producing Legal or Similarly Significant Effects[10] *These automated decisions do not typically produce such effects. Instances where they might produce such effects are contextual and should be determined on a case-by-case basis.*	• Decisions ensuring network, information and asset security, and preventing cyber-attacks • Decisions to sandbox compromised devices for observation, restrict their access to or block them from a network • Decisions to block access to malicious web addresses and domains and delivery of malicious emails and file attachments • Decisions for fraud detection and prevention (e.g., anti-fraud tools that reject fraudulent transactions on the basis of a high fraud score) • Decisions of automated payment processing services to disconnect a service when customers fail to make timely payments • Decisions based on predictive HR analytics to identify potential job leavers and target them with incentives to stay • Decisions based on predictive analytics to anticipate the likelihood and nature of customer complaints and target appropriate proactive customer service • Normal and commonly accepted forms of targeted advertising • Web and device audience measurement to ensure compliance with advertising agency standards (e.g., requirements not to advertise foods high in fat, sugar and sodium when the audience consists of more than 25 percent of children)

With the essential use of machine learning and AI to process the increasing amount of data, profiling is no longer an option but a reality in relation to many processing functions. As with the processing of special category data, profiling should not be prohibited per se, but should be permitted with safeguards, and a flexible approach to accommodate the evolving technology, practices and customer expectations in this area.

E. **<u>Anonymisation</u>**

1. *Proposal: Placing a test for anonymization onto the face of legislation*

CIPL supports DCMS' proposal to incorporate a test for anonymised data into an updated UK data protection regime. However, CIPL proposes basing such a test on the US FTC model[11] for anonymisation rather than on Recital 26 of the UK GDPR or on the wording of the Explanatory Report accompanying Convention 108+. The FTC model requires reasonable technical anonymisation, coupled with a legal prohibition against re-identification (with exceptions for when re-identification is necessary) and contractual and administrative safeguards against re-identification. CIPL believes that this combination of

[10] Another kind of decision in the category of not producing legal or similarly significant effects that was not included in this list at the time, but that should be included going forward, are decisions to surface content to specific users, i.e., decisions relating to personalizing content based on a user's demonstrated interests.
[11] United State Federal Trade Commission Report "Protecting Consumer Privacy in an Era of Rapid Change -- Recommendations for Business and Policymakers", March 2012, at pp 20-21, available at https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

safeguards provides an effective and practical standard given that technical measures alone are not sufficient to ensure true anonymization. Basing an approach to anonymization on theoretical rather than practical standards creates a "no go" zone for anonymous data. This standard could provide a safe harbour for organisations looking to use previously identifiable data for research and other socially beneficial purposes.

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

A. Reform of the Accountability Framework

1. *Proposal: Implementing a more flexible and risk-based accountability framework which is based on privacy management programmes.*

CIPL welcomes the proposal to strengthen accountability by requiring organisations to implement a privacy management programme, tailored to their processing activities. The goal of accountability is to ensure that organisations implement appropriate policies, procedures and controls to process data responsibly and to enable organisations to implement such governance measures in ways that are appropriate and proportionate to the risks involved. It is not intended to burden organisations with a string of requirements that may not be relevant to the processing at hand or deliver no benefit to data subjects.

CIPL appreciates that DCMS has outlined specific elements that privacy management programmes should cover within the consultation, including leadership and oversight measures, risk assessments and procedures to monitor and verify the effectiveness of the programme. Indeed, CIPL has written extensively about the essential elements of accountability and recommends that the UK consider such elements in framing any specific outcomes to be achieved by the implementation of privacy management programmes.[12]

Moreover, CIPL agrees that further regulatory guidance on the implementation of privacy programmes that sets out regulatory expectations and dispels uncertainties about the operation of a new privacy programme requirement would be useful. Such guidance should build upon the work of the ICO's Accountability Framework.

[12] See the following CIPL White Papers "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society", July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf; Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability, July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf; Q&A on Organisational Accountability in Data Protection, July 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_q_a__3_july_2019_.pdf; and What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework, May 2020, available at https://www.informationpolicycentre.com/organizational-accountability.html.

2. *Proposal: Removing and amending various requirements in the current accountability regime.*

DCMS proposes to remove and amend several requirements set out in current legislation to support the implementation of a new accountability framework. This includes the following requirements: (a) appointing a data protection officer, (b) undertaking data protection impact assessments, (c) undertaking prior consultation with the Information Commissioner's Office, (d) maintaining records of processing, (e) breach reporting requirements.

CIPL supports enabling flexibility for organisations in implementing accountable privacy management programmes which reflect and are suited to the wide range of business structures and operations. However, it is important that any changes to the current rules be clearly explained and the requisite standard for compliance delineated to prevent stakeholders viewing any changes as a dilution or an abandonment of EU-specific data protection concepts introduced by the GDPR (which is not the case under the proposals) and to avoid a situation where flexibility for organisations results in a lack of clarity as to which actions to take to enable accountability. Moreover, it would be helpful if any changes could be presented as alternatives to the EU GDPR approach so that organizations that have implemented the EU requirements do not have to bifurcate their compliance programmes.

CIPL recommends that DCMS take the following into consideration:

- Privacy programmes can go above and beyond what is required by law and should be incentivized to do so. Thus, DCMS should make clear that the proposed new approach to accountability is designed to enable flexibility for organisations to achieve the necessary compliance outcomes where certain heretofore required measures are burdensome without any consequent benefits. Moreover, multinational organisations should be allowed to continue to implement the requirements of the existing regime, such as conducting DPIAs, maintaining records of processing, and designating a DPO as they deem appropriate under the circumstances. Indeed, this is the premise of the accountability approach – to enable organisations to make their own decisions with regard to how they handle personal data to achieve the best outcomes for the business and the best protections for individuals through a flexible data protection framework. A multinational organisation may be inclined to adopt a more onerous or restrictive standard and apply it globally (one-size-fits-all) rather than conduct a country-by-country analysis which is perfectly acceptable if this approach works best for the organisation.

- Data Protection Officer (DPO): DCMS should make clear that the proposal to remove existing requirements to designate a data protection officer does not displace the requirement to designate a suitable individual(s) or role to be responsible for the privacy management programme and for overseeing the organisation's data protection compliance. Moreover, DCMS should highlight that it recognizes that organisations have different set ups when it comes to the designation of a responsible person/role for data protection compliance. It may fall under the remit of a DPO, a CPO or chief data or trust officer. The goal is for organisations to assign responsibility for the privacy function in an organisation, and to empower that individual/function to carry out their tasks effectively. While this may be obvious for organisations with a mature privacy culture, it may not be the same for those who are less well resourced or mature in this regard.

- Data Protection Impact Assessment (DPIA): DCMS should clarify that its proposal to remove the requirement for organisations to undertake a DPIA displaces the formal and sometimes rigid requirement to conduct such assessments under the current regime, but that it very much envisions and would require organisations to continue to assess the risks and benefits of their processing activities and to be able to demonstrate these risk assessments to regulators. This would re-emphasize the need for companies to still consider the risks, but to do so in a more sensible and targeted fashion rather than when specific circumstances outlined in the law require.

- Prior consultation with the ICO: DCMS should promote constructive engagement and innovative regulatory tools, such as data protection sandboxes, in removing a requirement to undertake a formal prior consultation with the ICO. The goal should still be to encourage collaboration between organisations and the ICO where it would be effective and beneficial.

- Record keeping requirement: DCMS should clarify that removing the record keeping requirement under Article 30 of the UK GDPR does not mean that organisations are not obliged to keep any records at all. As DCMS has noted in the consultation, any new requirements would still require certain records to be kept, but organisations will have more flexibility about how and where to do this, in a way that reflects the volume and sensitivity of the personal information they handle, the types of data processing they carry out, and the structure of the organisation. Incorporating privacy into existing business operations and maturing these to include a privacy lens is an essential element of ensuring a culture of privacy compliance rather than siloed tick-box compliance.

- Article 14 Notices: It would be helpful to clarify that the provisions of Article 14 do not require individual notices, as this may be not be possible for organisations processing data on behalf of third parties where they do not have individual contact details. Instead, it should be sufficient to have published an accessible and clear notice for non-marketing/non-advertising processing of indirectly acquired data.

- Please also refer to the additional points included in the Appendix hereto summarizing key points made at recent CIPL industry roundtables with DCMS on the UK's data reform proposal, specifically the points made on privacy management programmes.

3. *Proposal: Changing the threshold for reporting a data breach to the ICO.*

CIPL agrees that over-reporting of data breaches since the introduction of data breach notification obligations has been a significant issue for organisations and regulators. CIPL supports the proposal to raise the threshold for breach reporting. Under the proposed standard, organisations must report a breach unless the risk to individuals is not material. The ICO should be encouraged to produce guidance and examples of what constitutes a "non-material" risk and produce examples of what is and is not reportable. Such an approach would:

- Resolve swamping regulators with unnecessary breach notifications;

- Curtail the trend of consumers initiating legal actions stemming from anxiety derived from unnecessary breach notifications; and

- Solve the problem of "notification fatigue" which can result in a loss of trust among individuals and prevent them from taking action where it is truly necessary to safeguard their privacy.

Similar to the European Data Protection Board's *Guidelines 01/2021 on Examples regarding Data Breach Notification*, the ICO should publish draft guidelines with example scenarios and provide organisations with the opportunity to submit comments prior to finalizing any such guidelines. This would allow organisations to understand what types of incidents the ICO views as reportable and why. Organisations would then have an opportunity to provide rationale or justifications for why certain types of incidents should or should not be viewed as reportable for the ICO's consideration as they work towards finalizing the guidelines.

4. *Proposal: Introducing a new voluntary undertaking process, similar to Singapore's Active Enforcement Regime.*

In line with CIPL's comments above on promoting constructive engagement between the ICO and organisations, CIPL supports the introduction of a new voluntary undertaking process that would enable organisations with demonstrable accountability practices to have the opportunity to implement a specific remediation plan to address any infringement of the law in lieu of enforcement action by the regulator. Once a violation has been identified, an organisation that is operating in good faith will likely be better equipped to decide on the most appropriate course of remedial action and regulators should give organisations the chance to cure any violations before pursuing more rigorous enforcement options. Of course, the ICO should consider each voluntary undertaking on a case-by-case basis. By analogy, this is an approach taken in relation to driving violations, where education in lieu of points/fine is the preferred route to address certain driving offences.

B. <u>Privacy and Electronic Communications</u>

1. *Proposal: Permitting organisations to use analytics cookies and similar technologies without the user's consent.*

CIPL agrees that it would be helpful to streamline the rules governing the use of cookies and to enable the use of analytics cookies without obtaining user consent. To the extent that analytics cookies are used to obtain general information about how many people visit a website, how they interact with it and what pages are most visited, CIPL believes that such information collection is generally low risk and should be permitted. Of course, CIPL agrees with DCMS that specific safeguards may need to be considered to ensure such processing does not result in a high risk to individuals.

2. *Proposal: Permitting organisations to store information on, or collect information from, a user's device without their consent for other limited purposes.*

CIPL supports any reform to the UK data protection regime that can enable organisations to store information on, or collect information from, a user's device without their consent for limited and legitimate purposes. CIPL supports an approach that would require transparency about the purposes of such processing to individuals and tackling the key concerns head on through the additional suggested safeguards or limitations on use (i.e., use of pseudonymisation, mandating that information is not used to build a profile of the user and/or requiring the use of transparency notices). Indeed, there exists a digital trust deficit around the use of tracking technologies precisely because individuals fear being tracked and

profiled for purposes which are unclear, illegitimate or unwelcome as they navigate the Internet and use apps.

While there is an opportunity for the UK to take a position on how organisations can enable targeted advertising in a way that is more privacy-enhancing and transparent, CIPL believes that the UK should not delineate a specific approach in a law, and issues around online behavioural advertising should be resolved by way of regulatory guidance. (For example, the ICO might be given the authority to approve (exempt from consent requirements) PETs or other innovative technologies that don't pose specific privacy concerns but that might otherwise require consent under PECRs.) There are several reasons for this:

- The online behavioural advertising landscape is complex, affects multiple stakeholders and is currently in a state of flux, with new changes and proposals by Apple and Google set to significantly change the way ads are targeted in future.

- Use of web browser settings to opt-out of targeted ads, while potentially a good solution, has faced push back and criticism from multiple players in the advertising ecosystem. Moreover, to be effective, such a solution requires coordination from different online services and, as such, can only work if there is alignment on the approach.

Chapter 3: Boosting Trade and Reducing Barriers to Data Flows

A. Adequacy

1. *Proposal: Approaching adequacy assessments with a focus on risk-based decision-making and outcomes.*

CIPL supports DCMS' proposal to base future adequacy assessments on the likelihood and severity of actual risks to data subjects' data protection rights and on an assessment of real-world outcomes of data protection regimes, rather than on a largely textual comparison of another country's legislation with the UK's legislation. However, CIPL highlights that a deviation from the current standard that necessitates essential equivalence of foreign laws with privacy protections under the GDPR regime may create political friction with the EU in instances where there is not current alignment on which countries should be deemed adequate. As DCMS frames an updated approach to adequacy, it should continue to engage with the EU and outline the benefits of a more flexible risk-based approach to transfers including on technical measures and safeguards, and why the UK approach achieves substantially similar data protection goals and outcomes as the EU approach.

2. *Proposal: Making adequacy regulations for groups of countries, regions and multilateral frameworks.*

CIPL supports DCMS' intention to explore whether to make adequacy regulations for groups of countries, regions and multilateral frameworks. Adequacy for a group of countries could be assessed collectively when such countries share data protection standards or adhere to a multilateral framework. CIPL believes that there is a possibility for the UK to work on interoperability with the APEC Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) standards and potentially find countries that adhere to the CBPR and PRP to be adequate in certain circumstances.

3. *Proposal: Amending the legislation to be clear that both administrative and judicial redress are acceptable as long as the redress mechanism is effective.*

CIPL supports, as part of the UK government's wider amending legislation, to clarify that administrative and judicial redress are acceptable as long as redress mechanisms are effective. Indeed, the UK is in a position to take a leadership role to develop global standards for government access to data and to resolve many of the open questions that followed from the European Court of Justice's decision in Schrems II.

B. Alternative Transfer Mechanisms

1. *Proposal: Exempting "reverse transfers" from the scope of the UK international transfer regime.*

CIPL supports the proposal to exempt reverse transfers from the UK's international transfer regime. This issue has been particularly problematic for organisations under the GDPR. It is questionable as to whether any risk is created for individuals by sending data received from one country back to that original country of origin. However, to the extent that any additional data is included with the data to be transferred, then consideration needs to be given as to whether the additional or transformed data is subject to the relevant international transfer requirements. CIPL highlights, however, that in exempting such transfers from the regime, a more comprehensive definition of transfer should be added to the law, and it should be clarified as to whether transfers cover transfers between legal entities (i.e., branches vs subsidiaries vs joint ventures etc.) within a group or to all transfers whether within or outside of a legal body.

2. *Proposal: Creating a new power for the Secretary of State to formally recognise new alternative transfer mechanisms.*

CIPL supports the creation of a new power for the Secretary of State to create new UK mechanisms for transferring data overseas or to recognise in UK law other international data transfer mechanisms, if they achieve the outcomes required by UK law. In that regard, CIPL encourages the inclusion or recognition of cross-border transfer mechanisms such as the APEC CBPR and PRP developed by the Asia-Pacific Economic Cooperation (APEC) forum. The CBPR are an enforceable corporate code of conduct or certification mechanism for intra- and inter-company cross-border data transfers reviewed and certified by an approved third-party certification organisation. The PRP are the equivalent specifically for transfers to data processors. The advantage of this system is that it allows transfers not only within a global corporate group (or within a group of enterprises engaged in "joint economic activity", such as under the BCR), but also between unaffiliated companies and to companies that are not CBPR-certified anywhere in the world. The CBPR-certified company remains liable for the protection of the information at the level of the originating APEC country and the CBPR, regardless of where or to whom the data is transferred.

3. *Proposal: Establishing a proportionate increase in flexibility for use of derogations by making explicit that repetitive use of derogations is permitted.*

CIPL believes that derogations should not be seen as stopgap measures (as all the other safeguards mandated by the GDPR would still apply). Derogations should be seen as essential transfer mechanisms where no other mechanisms apply, and data users should be able to rely on applicable derogations without prior regulator review or permission. In this regard, CIPL welcomes DCMS' proposal to provide more clarity and a flexible approach with respect to derogations. The interpretation of derogations should be made in the context of identified risks to data subjects.

Chapter 5: Reform of the Information Commissioner's Office

A. Strategy Objectives and Duties

1. *Proposal: Introducing a 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.*

CIPL cautions DCMS against introducing powers for the UK government to set the strategic direction of the Information Commissioner's Office. There is concern among several stakeholders that some of the proposed reforms would interfere with the ICO's ability to operate independently. CIPL believes that the UK government should communicate its own priorities to the ICO for consideration in setting its own strategic objectives but deciding the ICO strategic priorities should largely be left to the regulator. As such, CIPL does not recommend introducing a requirement for the ICO to respond to the government's statement of strategic priorities and to explain whether and how its work addresses those priorities. The ICO may wish to do so independently, through an official statement or in its annual report, but this should not be mandated.

The independence of the ICO is a fundamental building block of its credibility and standing within and outside of the UK, and this should be supported by government. The ICO must be able to hold government to account if it is to have credibility with business and the public. Moreover, the independence of the regulator is one of the foundational aspects of EU adequacy reviews. Such a proposed change may threaten the UK's continued enjoyment of EU adequacy and potentially with other adequate jurisdictions. With respect to the importance of the data protection regulator's independence, it may be instructive for the UK government to consider the EU Commission's focus on the issue of independence with respect to the U.S. Ombudsman's for the EU-US Privacy Shield (given that the US executive branch appoints the Ombudsman).

2. *Proposal: Introducing a new duty to cooperate and consult with other regulators, in particular those in the Digital Regulation Cooperation Forum (DRCF).*

CIPL supports introducing a duty for the ICO to cooperate and consult with other DPAs and sectoral regulators both in the UK and around the world. Cooperation and collaboration among different regulatory bodies is an essential element of ensuring regulatory coherence across sectors and for building understanding and best practice across jurisdictions. As data protection laws continue to be adopted and updated in jurisdictions across the globe, it is increasingly important for regulators to share their experience and best practice. Data protection legislation is in its infancy in some jurisdictions and is maturing through multiple iterations in other jurisdictions. Mutual recognition, building trust in international data transfers and ensuring a consistent approach to key legislative measures are the desired outcomes of regulatory cooperation and collaboration, recognizing the reality that we live and operate in a global environment, where the interaction with other regulatory regimes is a daily reality for individuals, businesses, governments and academia. The ICO is already carrying out such a duty as it is an active participant within the DRCF and a member of many international privacy fora, including the Global Privacy Assembly, the Global Privacy Enforcement Network and the Common Thread Network. The opportunity to both learn from other regimes and to share best practice is an essential element of building

an environment of trust and understanding between DPA's globally, and to helping instill confidence in the capabilities and expertise of the UK ICO as a world-leading regulator.

The DRCF model is already being copied in other jurisdictions (e.g., the Dutch Digital Regulation Collaboration Platform), and is important to ensure regulatory coherence. We would recommend that the duty to cooperate and consult with other regulators is recognized as being a mutual obligation within with DRCF to ensure that this is not a one-way obligation, given the many touch-points of personal data across the regulatory spectrum.

3. *Proposal: Introducing a duty for the ICO to have regard for economic growth and innovation, competition and public safety when carrying out its functions.*

While CIPL supports the general premise of the ICO considering other important interests in discharging its functions, including in the area of economic growth, competition and public safety, CIPL cautions that any proposal must be sufficiently specific and clarify what would be expected of the ICO in doing so. The delineations between these areas are becoming increasingly complex and the ICO should retain flexibility to work through these issues with other regulators, industry, academia, law and policy makers and maintain its independence to deal with issues concerning the intersection of these areas and data protection in the way it best sees fit. As such, any proposal to include such a requirement in the updated UK data protection regime should be framed broadly and flexibly to allow the ICO to prioritise accordingly.

4. *Proposal: Introducing a requirement to give the Secretary of State the power to approve codes of practice and complex and novel guidance.*

As discussed above, maintaining the ICO's independence is of utmost importance for ensuring its effectiveness, both domestically as well as globally *vis a vis* its foreign counterparts and the various international groupings of data protection authorities. A requirement to seek approval from the Secretary of State for new codes of practice or regulatory guidance is inconsistent with the ICO's status as an independent data protection authority. However, the ICO might be given an option to consult with the Secretary of State on such issues when it deems such consultations to be helpful and appropriate.

5. *Proposal: Introducing a requirement for a complainant to attempt to resolve their complaint directly with the relevant data controller before lodging a complaint with the ICO.*

Under the GDPR, regulators have reported an exponential increase in the number of consumer complaints they have received. Many regulatory bodies have become overwhelmed with a plethora of complaints, many of which have been resolved by directing data subjects to contact the data controller in question. CIPL supports introducing a requirement that requires organisations to be the first port of call to resolve consumer complaints before they are escalated to the ICO. This would not only relieve the complaint-handling burden on the ICO and achieve faster outcomes for individuals, but also, increase the accountability of organisations. It may also be helpful to allow organizations to incorporate addressing privacy complaints within an organisations' broader complaints management process, as it is often the case that privacy complaints are triggered by or require the resolution of non-privacy issues.

APPENDIX:

CIPL Roundtable Takeaways on UK DCMS Consultation on Reforms to the UK's Data Protection Regime

On October 13 and 14, 2021, CIPL held two roundtables where its members shared their views on the UK Data Reform proposals (the "Reform"). This report provides a summary of key considerations and takeaways with respect to four chapters of the Reform proposals.

Chapter 1: Reducing Barriers to Responsible Innovation

CIPL members believe the Reform is effective in terms of innovation, but should further streamline certain administrative rules. By doing so, it will be a role model for other jurisdictions.

Not everything should be a part of the regulation. The UK Information Commissioner's Office (the "ICO") also has a key role to play in adopting guidance to enlighten best practices.

1. **Scientific research and lawful ground for processing**:

- CIPL members welcome the proposed **open and flexible definition** of scientific research as it is beneficial to the research community and society in general. Scientific research is dynamic by nature and relies increasingly on AI. Privacy regulation is not only about protecting individuals' rights but also about balancing the rights of individuals with other societal interests, including scientific research. In the absence of an open and dynamic definition, the Reform would eventually exclude many areas of research that are beneficial to society.

- The definition of scientific research should **not include a requirement of investigating a stated hypothesis**, because very often the point of AI-based research is to generate new hypotheses (i.e., the research comes before the hypothesis, contrary to the traditional approach, where the hypothesis typically precedes the research).

- The creation of a separate **lawful ground for scientific research** promotes certainty and consistency. CIPL members warn however that departing too much from the EU GDPR can add complexity to the processing activities of multi-national organisations that would have to deal with two different legal regimes.

- CIPL members would undertake scientific research activities with more legal certainty if the regulator clarified the expected **safeguards** (e.g., the high standard of anonymisation eliminates the possibility of any data being considered anonymous).

- Private entities should be considered as contributing to the **public interest** when public and private organisations are working collaboratively on research projects. Equally, the research

must be seen through a broad lens, with privately funded and commercial research and development equally important and needs to be enabled in the law.

- GDPR's narrow approach to defining **consent** is not useful nor adaptable for research activities. Individuals should be able to provide broad consent in the context of research activities.

  The GDPR **compatibility test** should be interpreted with more flexibility in the research context. Relying on a presumption of compatibility would help to foster research.

- There is a lack of clarity on the interplay between Article 6 and Article 9 of the GDPR when health data (sensitive data) is processed and whether both articles apply cumulatively. It is difficult for the industry to determine the **correct legal bases** as scientific research only relates to Article 9 but not Article 6.

- CIPL members regret that some **Ethical Review Committees** go beyond their strict ethics review role and venture into interpreting certain GDPR rules, without real expertise or understanding of the whole GDPR framework. This creates uncertainties and subsequently restricts scientific research.

2. **Legitimate interest lawful ground for processing**:

- There is strong support for the proposal to clarify legitimate interests via a **whitelist** and to foster better implementation of this ground for processing. However, CIPL members consider that the list of legitimate interests should not automatically be deemed to meet the balancing test. Organisations will still need to do a risk assessment to identify the appropriate mitigations. Thus, the list should **list potential legitimate interests that are subject to necessary mitigation based on risk assessments.**

- In addition, it should be considered if it is possible to create a white list of low-risk legitimate interest processing activities that will not generally require any further balancing or risk assessment, subject to exceptional circumstances in which the regulated entity would have reason to believe that a risk assessment to identify proper mitigations should be undertaken nonetheless.

Chapter 2: Reducing Burdens on Businesses and Delivering Better Outcomes for People

1. **Privacy management programmes**

- CIPL members understand and welcome that the Reform is designed to strengthen accountability via an outcome-based and risk-based approach. They stress, however, that greater flexibility may lead to misinterpretation by organisations. In that regard, CIPL members suggest that further **clarification be provided to specify the outcomes** and ensure

there are at least minimum standards. Otherwise, there is a risk that businesses will not understand which actions to take.

- **Effective accountability needs credibility, understandability and transparency**. It is important that organisations and data subjects understand regulatory expectations. In addition, regulators and data subjects should be able to analyse to what extent organisations are satisfying those expectations.

- Some CIPL members highlight that large organisations may wish to **continue with the existing regime, especially maintaining DPIAs, DPO role, records of processing,** rather than a new accountability approach in the UK because they have already improved and implemented well-established privacy management programmes internally. At the same time, the Reform would not prevent organisations from going above UK law requirements.

- Some CIPL members believe that the envisioned accountability framework may create impediments for **SMEs**. However, they acknowledge that some of the Reform proposals (such as the legitimate interest proposal) will help reduce burdens on businesses while enhancing protections for individuals. The Reform could go further, for example, by setting pre-set criteria or enabling the regulator to whitelist processing activities (e.g., for payroll) or clarifying what constitutes a low-risk processing activity. These measures would assist SMEs' compliance with the rules.

- There is a risk that some of the proposals around accountability and Privacy Management Programme may not be understood well by the industry and UK may be seen solely as abandoning the EU concepts of DPIA, DPO, records of processing, rather then strengthening accountability and making the system more effective (which we recognize is not the case). This requires careful wording and explanation in the proposals.

2. **<u>Removing specific mandatory compliance requirements</u>**

- CIPL members question how far some of the Reform proposals should go in light of the criticism the UK could face. The Reform should **strike a balance** between organisational flexibility to achieve compliance and regulatory guidance for organisations. In that regard, the Reform should indicate what needs to be achieved rather than how it needs to be achieved. This should be supplemented by pragmatic guidance from the ICO.

- Regarding the role of the **data protection officer (DPO)**, organisations have different set-ups when it comes to the designation of a DPO. Having clear illustrations and guidance for the role and responsibilities of a DPO would be constructive and beneficial for organisations.

- There could be some **unintended effects** of removing some compliance requirements. For instance, removing the recordkeeping requirement may lead organisations to not keep any

records at all. Similarly, removing the DPIA requirement by default may create a risk for companies in the long term, especially considering the scalability of data processing. This may also affect public confidence that also relies on recordkeeping and DPIAs. Hence, having minimum standards would be more beneficial to organisations.

- Some CIPL members believe that **charging a fee for SARs** may not be appealing for data-driven business models because it can impact public trust and transparency. Those companies have already invested in technologies to run SARs efficiently and effectively, and they would not prefer to lose the incentive to improve their individual rights systems.

- There is a support for the proposal to raise the threshold for **breach reporting** for UK-based organisations operating in the UK. This can help resolve swamping regulators with unnecessary breach notifications. It would also curtail the trend of consumers initiating legal actions stemming from anxiety derived from unnecessary breach notifications. CIPL members ask however for international coordination, rather than regulatory competition, between DPAs for situations where breaches affect multinational organisations with multi-country data processing operations.

- Some CIPL members suggest the Reform streamline rules governing the **use of data that is in the public domain**, such as government records or other public domain data.

3. <u>Privacy and Electronic Communications</u>

- CIPL members agree that it would be helpful to streamline the rules governing tracking cookies by taking into account the fact that most cookies create **low risks** to individuals. A specific approach is needed only in relation to cookies that raise high risks for individuals.

- There is a strong support for expanding the use of **analytic cookies** without the need to obtain consent.

- The PECR is **not part of the EU adequacy assessment** now. This provides an opportunity to reform the rules governing cookies through a streamlined standard that can become a global compliance standard.

- CIPL members believe that the Reform could be improved by **incentivising privacy enhancing technologies**.

- There is acknowledgement that cross-site tracking in the advertising context undermines digital trust and confidence. The Reform provides the **opportunity to take a stance on how organisations can enable targeted advertising in a way that is more privacy enhancing** and transparent (by setting a standard on transparency and choice for instance).

- Generally, the proposal should **encourage innovation**, for instance by broadening the use of the regulatory sandbox similar to Singapore's approach. Many companies are not willing to move forward with certain innovations due to a fear of infringing the law. Broadening the regulatory sandbox would also attract startups to engage in data driven projects in the UK market. Simultaneously, it will also benefit consumer protection because innovations will be tested in the regulatory sandbox in advance of their release into the market.

Chapter 3: Boosting Trade and Removing Barriers to Data Flows

- The UK is in a position to take a leadership role in the OECD and other fora to develop global standards for **government access to data**.

- CIPL members welcome the flexible approach for **adequacy decisions**. Nevertheless, this may create political friction with the EU in instances where there is disagreement on which countries should be deemed adequate. The UK should continue to engage with the EU on the topic of adequacy and outline the benefits of a slightly more flexible approach and why it still achieves the same data protection goals as a more stringent one.

- The standard for adequacy and essential equivalence as defined by the CJEU sets a very high threshold. Nevertheless, CIPL members believe the UK is in the position to work on **interoperability with the APEC standards** to create globally interoperable standards.

- The Reform should revamp the **BCR process** to make it more efficient, flexible and less time-consuming in terms of the procedure for BCR approval by the ICO. The current timeframes in the EU are unacceptable and there is hope that the ICO may be more agile in dealing with UK applications only. Companies view BCR as a true accountability framework that goes beyond just data transfer mechanism, and establishes a group-wide effective privacy management programme. Companies with approved BCR should be able to transfer data between one another without having to rely on additional transfer mechanisms. The Reform should also work on making BCR more attractive for SMEs.

- CIPL members welcome the exemption of reverse transfers from the scope of the UK international data transfer regime. The EU should follow a similar approach. Some CIPL members request that **a transfer** be better defined and clarity added as to whether it covers legal entity transfers or physical transfers.

- In certain circumstances, derogations are the only way to a achieve data transfer. CIPL members believe that **derogations** should not be seen as stopgap measures (as all the other safeguards mandated by the GDPR would still apply). Derogations should be seen as essential transfer mechanisms where no other mechanisms apply. CIPL members would welcome further clarification and a more flexible approach. The interpretation of derogations should be made in the context of risks to data subjects.

- CIPL members would be in favour of **interoperability in relation to foreign certifications**. Such certifications could be considered to meet the core principles of UK law and get recognition from the ICO.

Chapter 5: Reform of the ICO

- CIPL members underline that the **independence of the regulator** is one of the foundational aspects of the EU adequacy reviews. It is important that the Reform maintain this principle in practice. In this regard, the EU Commission's consideration of the U.S. Ombudsman's independence (given that the executive branch appoints the Ombudsman) is an example for the UK government to consider while working on the ICO's independence.

- CIPL members welcome the expansion of the ICO's duties to **account for other inter-connected government objectives, such as competition, innovation and public safety**. However, CIPL members ask for further clarification and consideration to ascertain the roles and responsibilities of the ICO when discharging its functions.