Delivered on 26 November 2020

Key Issues and Questions Regarding the UK's Data Regulatory Regime

Summary of input provided during the 7 October 2020 CIPL-DCMS Senior Privacy Leaders Virtual Roundtable No. 2 with DCMS on the UK's Data Regulatory Regime

Below is a summary of the key CIPL messages on the UK data regulatory regime as well as specific points, issues and questions raised and input provided by CIPL members during the 7 October 2020 CIPL-DCMS Senior Privacy Leaders Virtual Roundtable No. 2 with DCMS: the UK's Data Regulatory Regime. They are organised (roughly) by topic/question of the roundtable agenda. Given the overlap between some of the topics/questions for discussion, certain topics were addressed multiple times, but from different angles. Thus, certain issues are addressed in more than one section below. Also given the overlap between the topics of this roundtable and the Senior Privacy Leaders Virtual Roundtable No. 1 with DCMS on International Data Transfers, this document refers to some of the key CIPL messages provided in the context of the roundtable 1.[i]

I. IMPROVING THE UK DATA REGULATORY REGIME

1. ***What are the biggest challenges and unfulfilled promises of the GDPR (i.e. provisions that did not work as intended, or have not yet been interpreted fully, thereby creating issues for organisations)? Is there an opportunity for the UK to improve its data protection regime using lessons learned from the GDPR as well as from the COVID-19 pandemic? Provide constructive examples and solutions.***
2. ***What are the helpful GDPR provisions that could be further implemented and developed to reach the GDPR's full potential (e.g. accountability tools such as certifications and codes of conduct; constructive engagement with stakeholders; transparent enforcement)? Why haven't these been fully realised yet? What can the UK do to promote them?***

Note: questions 1 and 2 were addressed altogether in the points below. For a more detailed discussion of the questions above please refer to the CIPL's Report on the 2 year Implementation of GDPR.[ii]

The UK should enable flexible, adaptable and broader interpretations of relevant GDPR provisions and concepts, so that they can continually evolve together with the technology they are intended to regulate while protecting individuals and their personal data. The UK should also leverage to their full extent all GDPR provisions, including the recitals and possible member state derogations.

A) Maintaining pragmatic accountability in the centre of the UK data economy

- Accountability is one of the foundations of the GDPR and the most promising regulatory and governance model for personal data in the digital economy and society. It means that organisations (i) take practical steps to comply with the GDPR requirements (such as implementing a data privacy management programme) and (ii) and are able to demonstrate, internally and externally, the existence and effectiveness of such steps taken.[iii] The UK should maintain and further develop this central role of accountability in the context of its digital economy and national data strategy, including in connection with regulating online harms, misinformation, content and protecting children.
- Some organisations believe that the requirement to "demonstrate compliance", coupled with a too literal interpretation of that requirement by the data protection authorities (DPAs), have

led organisations to systematically over-document their data processing decisions, processes and procedures. This has taken a corresponding toll on their ability to focus on developing more practical solutions and measures that actually enable accountable uses of data. The UK should interpret accountability in a pragmatic manner and clarify that it is about giving effect to corporate digital responsibility rather than excessive record-keeping and compliance tick-box exercises.

B) Clarifying the meaning of a risk-based approach

- The GDPR's risk-based approach is central to the principle of accountability and to the proper functioning of a data protection legal regime, as it enables organisations to calibrate their compliance measures based on the risks and harms to individuals associated with their data processing activities. This results in better allocating compliance and mitigation resources when the risk to individuals is higher, i.e., in more targeted and tailored privacy protections.[iv]
- Unfortunately, some EU DPAs have not yet fully acknowledged the concept of a risk-based approach and interpret some of the GDPR provisions in a way that goes against such principle. This is the case, for instance, where DPAs act as though consent has a privileged position over other legal bases for processing. Also, much of the existing European Data Protection Board (EDPB)'s guidance does not take into account a risk-based approach and ability to callibrate compliance based on the risks to individuals. The UK should continue to apply its pragmatic view towards this concept of a risk-based approach in data protection—for instance, by acknowledging that processing risks are context-specific rather than static across and between entire industry sectors.
- The UK should also clarify some aspects of the concept of a risk-based approach, as well as any associated regulator expectations:
    - The types of harms to individuals that must be taken into account when doing the assessment;
    - How to balance risk to individuals's privacy against other fundamental human rights in line with the GDPR's recognition that the right to the protection of personal data is not an absolute right and that it must be balanced against other fundamental rights, in accordance with the principle of proportionality; [v]
    - How to balance low or trivial privacy risks against substantial benefits to individual(s) or society of a particular processing; and
    - How to avoid unnecessary reticence risk, i.e., the risk of not engaging in a particular processing operation where the processing would be low risk and the forgone benefits would have been high.

C) Preventing over-notification of data breaches and clarifying the notification process

- The lack of clarity concerning the GDPR data breach notification requirements, in particular of the concept of high-risk processing, resulted in organisations over-notifying data breaches to DPAs for fear of sanctions for failure to notify. This resulted in an unecessary increase of DPA workload with cases that were not high-risk, making it more difficult for DPAs to identify high-risk cases requiring immediate and deeper attention. The UK should clarify the requirements and intended outcomes for notifying data breaches, not only relating to the concept of high-risk data processing but also other issues such as notification requirements in the processor-

controller relationship, notifying suspected data breaches, timeframes for notification, and additional industry or sector-specific security requirements (especially in a global environment).

D) Rethinking the interpretation of the legal bases for processing in a way that comports with evolving technologies and business models and promotes effective data uses

- All GDPR legal bases are on equal footing and none of them is privileged over the other. [vi] However, policymakers and regulators in Europe and globally too still appear to give more weight to consent over other legal bases, believing that it empowers individuals and gives them control over their own data. Given the high bar for obtaining valid consent in the GDPR, organisations, however, cannot always rely on consent to process personal data in an increasing number of modern data processing contexts, including when data is processed for public good. Nor can individuals be expected to protect themselves by withholding or providing consent in a complex digital economy and society.
- The UK should re-think the interpretation of legal bases for processing in order to encourage organisations to use a wide variety of legal bases to lawfully process and share personal data. Organisations should be able to rely on more agile and flexible legal grounds than consent, such as legitimate interests, vital interests and public interest. They should also be able to rely on legal exemptions such as processing of data for research, as well as further processing personal data for compatible purposes.[vii] These have become even more relevant in the COVID-19 context and should be more broadly enabled.

E) Unlocking the potential of data portability

- Although provided for by article 22 of the GDPR, the right to portability has not been used by individuals, nor has it been promoted by organisations in part due to lack of a common technical and accountability framework to share data between service providers. The UK should consider how the right to data portability can empower individuals while acting as a catalyst for increased competition in the data economy through increased accountable data sharing. When doing so, the UK should be mindful to interpret this right in a way that does not interfere with intellectual property rights or undermine trade secrets of organisations.

F) Promoting privacy by design and data protection impact assessments (DPIAs)

- Privacy professionals recognise that privacy by design and DPIAs have helped them in their efforts to embed privacy into the corporate culture of their organisations, as well as to mitigate risks to individuals and to organisations. In order to work effectively, these activities should be integrated into enterprise processes, such as development lifecycles, product approvals, due diligence, third party governance. This encourages proactive engagement between the individuals responsible for data privacy within the organisation and other corporate functions and internal stakeholders. The UK should clarify to organisations the benefits of having data privacy as part of their corporate culture and promote privacy by design and DPIAs as mechanisms that contribute to an effective data privacy culture.

G) Promoting the use of pseudonymous, anonymous and de-identified data

- Under the GDPR, pseudonymised data is still considered personal data and is therefore subject to all GDPR requirements. However, the risks to individuals associated with the processing of pseudonymous data are much smaller compared to the risks of general data processing. The

use of pseudonymous as well as anonymous and de-identified data is critical for organisations to conduct data analytics in a privacy protective way, as well as to share data with other organisations or to use data for new purposes, including those for the public good. The UK should re-think the interpretation of pseudonymous, anonymous and de-identified data and incentivise their use under a risk-based approach. Pseudonymous data could be subject to a lighter legal regime, based on risk assessment and considerations.

H) Clarifying that the provisions that enable personal data to be processed for research purposes apply to both private and public sector organisations

- The GDPR allows organisations to further process personal data for research or statistical purposes (Article 5.1(b)), as long as appropriate safeguards are put in place in order to respect the principle of data minimisation, such as pseudonymisation (Article 89.1). The GDPR also allows for member states to provide derogations that would exempt data subject rights from applying to data processed for research and statistical purposes (Article 89, 2). However, certain organisations, in particular private organisations and SMEs, are still unsure whether and in what cases they can rely on these GDPR exemptions.
- The COVID-19 pandemic has made clear the importance of using personal data for research and statistical purposes for social good. Data processing for research purposes and data analytics is also key for innovation and the development of new and emerging technologies such as artificial intelligence (AI). The UK should acknowledge that the GDPR research exemption applies to both public and private organisations, and should clarify in what instances such organisations can use data for research, statistical and analytics purposes.

I) Promoting certifications and binding corporate rules (BCR) as accountability and interoperability mechanisms as well as international data transfers mechanisms

- The GDPR allows for certifications to be used as (i) mechanisms to enable international data transfers, and (ii) a tool to demonstrate compliance with the GDPR. At this stage however, no certification is available in the EU. The UK should should prioritise the development of certifications, recognise BCR as a form of certification, and recognise certifications as true accountability mechanisms by enabling organistaions to certify their privacy management program (accountability), as opposed just individual services, products or processing operations.
- As immediate steps, the UK should set up a simple, pragmatic and scalable certification framework and promote certifications certifications and their benefits among UK businesses. The UK should also develop this framework with an eye to similar existing global schemes to ensure interoperability, such as certifications provided by the International Organization for Standardization (ISO), the APEC Cross-Border Privacy Rules (APEC CBPR) System, binding corporate rules (BCR) and others.
- The UK should also further unlock the potential of BCR as an international data transfers tool. For instance, organisations with approved BCR should be able to share data among themselves without having to rely on any specific transfer tool as they already comply with the highest data protection standards. The same reasoning should apply to transfers between companies with approved BCR and certified companies or companies adhering to a code of conduct.

J) Streamlining the approval process for codes of conduct

- Similar to certifications, the GDPR allows for codes of conduct to be used as a tool to demonstrate compliance with the GDPR. It also enables organisations of the same industry sector and organisations that work in similar technologies across different sectors (such as blockchain, digital interface) to use codes of conduct to devise more agile, innovative and tailored compliance solutions.
- Organisations are, however, finding it difficult to obtain approval for codes of conduct and reported that certain DPAs are imposing high thresholds that go beyond the GDPR requirements. It is also a challenge to identify and finance organisations that will be responsible for monitoring compliance with the codes. The UK should streamline the approval process for codes of conduct and work with organisations and professional associations to help them understand their benefits and why they should invest in such mechanisms.

K) Ensuring alignment between the GDPR and ePrivacy

- The current disparities between the GDPR and the ePrivacy rules causes confusion for organisations and prevents them from using data for legitimate purposes and take fast decisions, especially in crisis contexts such as COVID-19. The UK should seek alignment between the GDPR and ePrivacy rules as they are applied and possibly updated in the UK.

L) Avoiding confusion between data ethics and data privacy

- The UK should be careful about creating the perception that data ethics is only a data protection or privacy matter. Data ethics involves many other concepts related to data governance and human rights that go beyond privacy. Limiting it to privacy places an unecessary burden on privacy officers and takes their attention away from operationalising privacy protections. It also creates the risk that data ethics boards pronounce on data privacy issues without having the right level of technical expertise[viii].

3. How can the UK mitigate concerns that a business-friendly approach towards the development of the data economy would be detrimental to individual protections, including personal data protection?

- Accountability provides many concrete benefits to all stakeholders—companies, privacy enforcement authorities and individuals. Benefits to companies include enabling data driven innovation, providing a reputational competitive advantage and generating trust. Such benefits, as well as the risk of enforcement, will motivate companies to properly implement accountability throughout their organisation. Encouraging accountable business practices is therefore not necessarily about taking a business-friendly position, but about enabling a consistently high-level of protection for individuals while also facilitating the development of the digital economy. Accountability does deliver effective protection and empowerment for individuals. For example, accountable organisations conduct risk assessments that lower the level of risks for individuals; implement enhanced transparency; put in place procedures for exercise of individuals' rights and complaints; and build other controls, processes and policies to implement legal requirements in a risk-based manner. Lawmakers and DPAs should thus provide additional incentives that encourage companies to adopt accountability measures, and should also reward companies that invest in privacy and accountability.

4. What mechanisms should the UK promote to enhance trust in the use of personal data in the public and private sectors (e.g. regulatory sandboxes; case studies developed by the UK Information Commissioners' Office (ICO); education campaigns)?

A) Accountability and data sharing frameworks

- Trust in data should be encouraged through frameworks that protect data but also enable access and responsible uses of data based on the related risks to individuals—such as accountability and data sharing frameworks. The UK should encourage the use and development of such frameworks (see Question I.2 above for why the UK should encourage accountability).
- In particular, the COVID-19 pandemic has demonstrated the importance of data sharing and highlighted the need for frameworks that provide legal certainty to public and private organisations that they can share data in a responsible and accountable manner. Such data sharing frameworks could cover, for instance, data governance, data sharing processes, due diligence processes, specific tech developments (e.g. common APIs, data sharing processes, etc.), as well as both personal and non-personal data.
- Data sharing, in particular in the public sector, is important to drive efficiencies, use of data for good and improve public services. As governments and public sector are also subject to data protection obligations, the UK should be extra cautious in holding them accountable to the UK data protection standards. Additional education and capability building initiatives would be welcome on this front.
- Data sharing is needed not only within the UK, but also across borders, in particular given that many of the organisations involved in developing technological solutions have a global reach. Part of the UK's work to promote data sharing will therefore be also educating governments and international bodies on the importance of data sharing and access to open data, as well as the problems that initiatives such as data localisation can cause to the digital economy (see response to Question III.1 below on data localisation).

B) Certifications, codes of conduct and BCR

- Certifications, codes of conduct and BCR are accountability mechanisms and, as such, are enablers of trust in the digital economy (see response to Question I.2 above). Organisations report that going through the process of obtaining certifications and BCR as well as joining codes of conduct help them verify the relevance of their internal processes and procedures. This enables them to demonstrate compliance to a number of stakeholders, including regulators, boards and executive committees, partners, clients and consumers—therefore generating trust in the ecosystem. As already mentioned above, the UK should recognise that certifications, codes of conduct and BCR are efficient accountability mechanisms and promote them to create a catalyst effect on the market.

C) Coordination among regulators and policymakers

- Trust is also about legal certainty. Organisations, however, face legal uncertainty when different regulators and policymakers have diverging expectations and provide diverging guidance and rules on overlapping topics—such as data privacy and competition, anti-money laundering, consumer law, cybersecurity. This makes it challenging for organisations who are faced with irresolvable conflicts of law while trying to innovate in the digital economy. The UK

should therefore promote better coordination and cooperation between all regulators and policymakers that have a role to play in the context of the UK National Data Strategy, in particular on topics such as data sharing, data management and new and emerging technologies.

D) Regulatory sandboxes

- Regulatory sandboxes in data protection are beneficial to organisations, DPAs, individuals and society and represent a good example of outcome-based smart regulation. Regulatory sandboxes provide a safe space for implementing, refining and testing innovative technologies and business processes with the guidance of a competent regulator.[ix] The UK ICO has successfully implemented a regulatory sandbox initiative in the data protection sphere[x]. The UK should encourage regulatory sandboxes to be organised not only in data protection but also in other areas relating to the UK National Data Strategy and high-risk areas such as fighting the COVID-19 pandemic. Organisations welcome regulatory sandboxes that cut across different areas of regulation, as they would also be a way to encourage cooperation among different regulators and streamline the regulatory review process by offering a one-stop-shop solution.

E) Case studies, practical guidance, template, tools

- Alongside fighting the challenges relating to GDPR implementation and promoting its helpful provisions (see responses to Questions I.1 and I.2 above), the UK should provide outcomes-based case studies, practical guidance, templates and online tools to organisations, in particular to SMEs, on the many topics that are part of its UK National Data Strategy. Organisations report that regulatory guidance in data protection is sometimes too extensive and legalistic, does not address their practical and operational needs, and does not show what good and bad look like. The ICO is seen as one of the most pragmatic DPAs globally and their guidance and tools are generally welcomed—such as the COVID-19 information Hub, the ICO Accountability Framework and the AI Framework.

5. ***How should the UK promote and encourage accountability and good faith compliance? Consider the mechanisms that could enable organisations demonstrate compliance with data protection principles and regulations (e.g. DPIAs used to demonstrate good data governance beyond risk-measurement; accountability frameworks; certifications).***

- The key to promoting organisational accountability is for the UK to take an outcomes-based approach to data protection regulation and enforcement. This means that the UK should focus on the impact of data processing on individuals with incentives for "desirable" outcomes and sanctions for "undesirable" outcomes based on risks, rather than on whether organisations follow prescriptive rules in a certain way. The UK should also provide clear guidance and examples to organisations on the outcomes they need to achieve, rather than how they have to achieve and demonstrate them.

- Such outcomes-based approach relies to a significant extent on constructive engagement between DPAs and accountable organisations. Prioritising the acknowledgment and encouragement of "desired" conduct over penalising "undesirable" conduct is a core principle of constructive engagement. More generally, regulators and law enforcers need to balance enforcement with engagement, thought-leadership, guidance, co-regulatory approaches

(such as codes and certifications) and sandbox initiatives, and not put too much emphasis on enforcement alone.[xi]

- There is a broad range of specific ways in which the UK could encourage broader implementation of accountability, such as:[xii]
    - Interpreting data protection principles and requirements through the lens of risk and more flexibly for organisations that demonstrate accountability (see response to Questions I.1 and I.2 above);
    - Allowing organisations that can effectively demonstrate accountability beyond pure legal compliance to pursue a broader range of reasonable and beneficial uses of personal data—such as through regulatory sandboxes (see response to Question I.4 above); and
    - Formally recognising demonstrated and/or certified accountability (such as accountability and data sharing frameworks, codes of conduct and certifications) as (i) a mitigating factor in enforcement actions and in assessing sanctions and/or levels of fines, (ii) evidence of due diligence when selecting data processors or service providers, and (iii) a formal cross-border data transfer mechanism (see responses to Questions I.2 and I.4 above).

II. BUILDING OUTREACH AND A POSITION OF GLOBAL LEADERSHIP FOR THE UK

1. How should the UK prioritise its multilateral engagement with regards to data protection and developing the data economy (e.g. ranking countries based on volume of data transferred; prioritise countries with the biggest economic impact for the UK; prioritise regions with significant economic potential, e.g. APAC; prioritise countries with developing data protection laws such as India and Brazil; prioritise specific fora such as the Global Privacy Assembly (GPA))?

- The COVID-19 pandemic has demanded not only private organisations, but also governments, policy-makers and regulators to prioritise their activities that bring the most beneficial outcomes for society. The UK government should apply the same pragmatism when developing its position of global leadership in the context of the data economy. It is important that the UK continue to be informed and current with developments in technology and business trends as well as with public expectations concerning the digital economy. This means prioritising its outreach efforts to the areas, regions and fora where their are bigger chances of successful outcomes in relation to the UK National Data Strategy.
- For instance, the UK should identify like-minded countries, economies and international bodies that can help shape and accelerate the responsible development of the global digital economy. Examples include other countries that also embrace a form of regulation that is centered around constructive engagement between regulators and regulatees, that also employ trust-enabling tools such as regulatory sandboxes (e.g. Singapore), and that have a similar understanding concerning key data protection concepts such as organisational accountability. Generally, the UK should address the topic of development of a global data economy in global organisations and fora, such as the G20, Organisation for Economic Co-operation and Development (OECD), World Trade Organisation (WTO), Council of Europe and the Global Privacy Assembly (GPA).

- The UK can also support the development of initiatives that are key for the global digital economy and for global interoperability, such as the APEC CBPR. When and if CBPR (and its companion certification for processors—the APEC Privacy Recognition for Processors (PRP)) are made available to non-APEC countries, the UK should join the CBPR system and help update and modernise it. It should simultaneously encourage and enable UK businesses to participate in this certification scheme and build effective interoperability tools that connect the CBPR to their counterpart UK/EU mechanisms, such as BCR, codes of conduct and certifications.
- Finally, the UK should leverage key global fora which it is already part of. For instance, the ICO has a leadership position at the GPA and should use this forum to encourage global privacy solutions and educate other data privacy regulators on topics related to constructive engagement, smart and outcomes-based regulation, as well as the importance of prioritisation and risk-based approach.

2. ***What are the objectives and opportunities for ongoing engagement between the DCMS and the ICO with their respective EU counterparts?***

- It is important to remember that companies subject the EU GDPR will need to continue to comply with it as well as with the rules and expectations of EU DPAs. The UK should seek integrating and harmonising th UK GDPR with the EU GDPR processes in order to help create the legal certainty around compliance obigations under both systems that UK businesses operating in the EU will need, and vice-versa. The UK should also work with EU policymakers to the extent possible towards a pragmatic interpretation and implementation of the EU rules that concern data and the digital economy. In particular, the UK should continue influencing and engaging with the EDPB and other EU regulators and policy-makers that are relevant in the context of the UK National Data Strategy. The ICO should continue its bilateral engagement with EU DPAs, as well as other EU institutions and policy-makers.

3. ***What are the objectives and opportunities for ongoing engagement between the DCMS and the ICO with the Organisation for Economic Co-operation and Development (OECD), in particular taking into account that the ICO's Deputy Commissioner has been appointed chair of the OECD's Working Party on Data Governance and Privacy?***

- The OECD has taken on the task to examine two important issues, which are both acting as an impediment to global data flows with trust: data localisation and excessive government access to data. The UK should encourage these initiatives and seek allies within the OECD to push the topics (at least the data localisation one) to be included in the review of the OECD guidelines. Just like in its bilateral trade agreement, the UK should seek to put some limitations to the data localisation attempts in countries across the world, which are members of OECD. We appreciate that the topic of governmental access to data is more complex and dependent on more factors. There is however also a need to address this topic in a multilateral fora, with a like-minded group of countries, so that excessive governmental access to data does not become an impediment to global data flows. This is particularly essential in light of the *Schrems II* CJEU decision. At the same time, it is important to preserve the need for democratic governments to be able to conduct surveillance and intelligence-gathering activities based on the rule of law and what is proportionate and necessary in a democratic society.

III. PROMOTING GLOBAL INTEROPERABILITY IN DATA PROTECTION

1. What are the most effective measures for the UK to fight the data localisation trend, in particular considering the impacts of the Schrems II decision by the Court of Justice of the European Union (CJEU)?

- Data localisation is at odds with current standards of access to information and with how the global digital economy must work to function properly. It is ultimately detrimental to businesses, the economy and governments. It can generate unintended consequences, such as serious impact on global communication, collaboration, research, fraud prevention and cyber security. It is expensive, duplicates data and creates data vulnerabilities. However, the world is trending towards dividing into localised and non-localised jurisdictions both through hard and soft law. Also, government departments and bodies are contractually requiring organisations to keep personal data localised and, in some cases, requiring data in the EU to be "repatriated" if there is a no-deal Brexit.
- There are several ways the UK can fight the data localisation trend:
    - Leverage existing international and regional fora (see response to Question II.1 and 3. above) as well as other communication channels to provide a strong voice and leadership against data localisation;
    - Engage bilaterally with like-minded countries and economies to andvance an anti-localisation message;
    - Provide thought-leadership concerning the negative impacts of data localisation as well as the benefits of free data flows for the global digital economy, such as through the promotion of research and studies as well as the publication of papers; and
    - Develop or participate in international and bilateral agreements that enable free data flows, encourage organisational accountability practices and prevent data localisation measures.

2. How can the UK promote global interoperability in data protection? What multi-lateral certification mechanisms or accountability frameworks could be leveraged and further developed for the purpose of global interoperability?

A) Building national data protection mechanisms with interoperability in mind

- As the UK advances its UK National Data Strategy, implements more flexible and adaptable interpretations of the GDPR requirements and builds data protection mechanisms, it should aspire towards interoperability between its own mechanisms and their global counterparts. Such interoperability encompasses not only interoperability between the UK GDPR and the EU GDPR (see response to Question II.2 above), but also interoperability with other overlapping global data protection regimes, accountability frameworks, and certifications. Many global organisations, for instance, design and map their global data privacy management programmes to one global standard that overlaps with various local data protection systems.
- The UK should create formal cross-recognition of such standards and systems, or bridge mechanisms between overlapping standards and systems. For instance, if organisations have

obtained a certification or take part in an accountability scheme that overlaps with the UK data protection requirements (e.g. BCR, GDPR codes of conduct and certifications, UK codes or certifications, CBPR, PRP, ISO Standards, etc.), the UK should validate such certification/participation rather than require the organisation to undertake each recognition or certification processes again under the UK law (and at substantial cost).

B) Promoting a global dialogue on interoperability

- The UK should proactively insert itself into the global dialogue and development processes regarding alternative multilateral transfer mechanisms and act as a catalyst for global interoperability. The UK could also leverage existing international fora when promoting such dialogue (see response to Question II.1 above).

C) Joining the CBPR system if and when it opens up to non-APEC countries

- Opening the CBPR to non-APEC countries is something that the APEC countries participating in the CBPR are actively pursuing. Joining the CBPR will enable the UK to help shape the expected updates both to the APEC Privacy Framework and to the CBPR that operationalise it, and to make the CBPR more interoperable with the GDPR requirements. The UK could also help drive more bridging between the CBPR and EU GDPR as well as other certifications (such as ISO certifications), codes of conduct and BCR in the future. It could also help drive interoperability with emerging data protection laws such as in Brazil and India.

D) Pursuing a role in the modernised Convention 108+

- The UK has ratified the Council of Europe Convention 108 and could also pursue a role in influencing the modernisation of Convention 108+ towards interoperability with global data protection regimes.

3. How can the UK leverage existing fora to promote global interoperability in data protection (e.g. ICO through the GPA and OECD's Working Party on Data Governance and Privacy)?

- *See responses to Questions II.1, II.2, II.3, III.1 and III.2.*

If you would like to discuss any of the comments in this document or require additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com; Markus Heyder, mheyder@huntonAK.com; Nathalie Laneret, nlaneret@huntonAK.com; or Giovanna Carloni, gcarloni@hunton.com.

---

[i] Key Issues and Questions Concerning International Data Transfers—Summary of input provided during the 24 September 2020 CIPL-DCMS Senior Privacy Leaders Virtual Roundtable No. 1 with DCMS on International Data Transfers, available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_key_points_and_messages__cipl-dcms_september_24_roudtable__9_nov_2020_.pdf>.

[ii] CIPL Response to the EU Commission's Public Consultation on the Evaluation of the GDPR, available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_eu_commission_consultation_on_gdpr_evaluation__28_april_2020_.pdf>.

[iii] CIPL has written extensively on the topic of organisational accountability. See for instance, the CIPL White Paper Organisational Accountability – Past, Present and Future, available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-

_organisational_accountability_%E2%80%93_past_present_and_future__30_october_2019_.pdf>, The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society, 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>, and the Q&A on Organisational Accountability in Data Protection, available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_organisational_accountability_%E2%80%93_past_present_and_future__30_october_2019_.pdf>. In particular, CIPL has written a report outlining how 17 leading organisations of different geographies, industry sectors and sizes have implemented the principle of accountability: What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework, available at <https://www.informationpolicycentre.com/organizational-accountability.html>.

[iv] CIPL has written about the concept of a risk-based approach in data protection in the following paper: Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR, available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf>.

[v] See Recital (4) of the GDPR "The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."

[vi] See more on CIPL's Response to the EU Commission's Public Consultation on the Evaluation of the GDPR, available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_eu_commission_consultation_on_gdpr_evaluation__28_april_2020_.pdf>, and on CIPL's white paper on Transparency, Consent and Legitimate Interest Paper – Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR, available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf>.

[vii] In its guidelines on contractual necessity, the EDPB unfortunately did not pronounce on the possibility offered by the GDPR to further process data for compatible purposes when the controller processed data on the basis of contractual necessity. See CIPL's response to the EDPB consultation on contractual necessity CIPL Comments on the EDPB's Guidelines on the Processing of Personal Data under the GDPR at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_comments_on_the_edpbs_guidelines_on_the_processing_of_personal_data_under_article_6_1__b__gdpr_in_the_context_of_the_provision_of_online_services_to_data_subjects.pdf>.

[viii] Such as for instance in the case of clinical trials where ethics committee tend to automatically consider that consent of the patient is required where these would rather fall under the scientific exemption of article 89 of the GDPR.

[ix] See the CIPL Regulatory Sandbox White Paper – Regulatory Sandboxes in Data Protection - Constructive Engagement and Innovative Regulation in Practice, available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_regulatory_sandboxes_in_data_protection_-_constructive_engagement_and_innovative_regulation_in_practice__8_march_2019_.pdf>.

[x] See the ICO Guide to the Sandbox, available at <https://ico.org.uk/sandbox>.

[xi] See the CIPL Regulating for Results Paper – Regulating for Results: Strategies and Priorities for Leadership and Engagement, available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement_2_.pdf>.

[xii] See the CIPL white paper Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability, 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>.