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

Below is a summary of the key CIPL messages on cross-border data transfers as well as specific points, issues and questions raised and input provided by CIPL members during the 24 September 2020 CIPL-DCMS Senior Privacy Leaders Virtual Roundtable No. 1 on International Data Transfers. They are organised 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.

I. THE CURRENT GDPR DATA TRANSFER REGIME AND MECHANISMS

1. ***How are the GDPR data transfers provisions currently working for organisations transferring data from the UK to the EU and vice-versa?***
2. ***What are the biggest challenges/obstacles at the moment for organisations to transfer data from the UK to third countries (EU and non-EU)?***
3. ***What are the most frequently used and helpful GDPR data transfers tools/mechanisms for organisations?***

- Adequacy, standard contractual clauses (SCC), binding corporate rules (BCR—controller and processor), derogations and the invalidated Privacy Shield have all been used by companies in the past and have been helpful. Different mechanisms are used to legitimise different data flows within the corporate group or with third parties (acting as processors or controllers). SCC appear to be the most widely used mechanism.
- The biggest challenge for organisations is not having sufficient legal certainty regarding how EU-UK and EU-third country data flows will be governed in the coming months and in the long-term, especially in the aftermath of *Schrems II*. The primary cause for this legal uncertainty is that data transfer rules and mechanisms have been vulnerable to disruption caused by legal challenges (e.g. with respect to the EU-US Privacy Shield and SCC).
- For some organisations, EU-UK data flows are a top priority. Most (but not all) organisations believe that maintaining/gaining UK "adequacy" must be the top priority for the UK government. However, some believe that from a business prioritisation perspective, UK adequacy is secondary to solving the real and global problems of data transfers, for which other mechanisms are better suited (see below).
- UK adequacy decisions with respect to third countries would be very helpful for organisations. The UK should explore sectoral adequacy, either for specific sectors where there is sectoral data protection legislation in the recipient country or for processing activities and transfers of personal data from UK to processors in other countries (e.g. India). In the latter case, the obligations on processors are more limited than on controllers and can, in any event, also be reinforced by controller-processor contracts.

- Absent UK adequacy, the focus should be on welcoming/establishing as many transfer mechanisms as are available under the law and pointing out ways to improve them. CIPL has advocated for global data protection laws to have similar and broad toolkits of data transfer mechanisms to drive convergence and make it easier for companies to use the same tools in all countries.
- The following are some specific examples of possible improvements to existing transfer mechanisms:
    - BCR should be able to be used for inter-company transfers between companies not in the same corporate family, if both have received approvals for their BCR. (The GDPR provides that BCR can be used to legitimise transfers between undertakings engaged in joint-economic activity).
    - SCC must be updated in light of the GDPR and of *Schrems II*. They must provide organisations with the ability to adapt them to their own contexts. The current SCC do not fit well with current transfer models—for instance, where there are multiple contracting parties (controller/processors), or with respect to transfers to sub-processors.
    - Codes of conduct and certifications for transfer purposes should be created (see more on improvements below).
- Organisations are concerned that the UK may not be able to break sufficiently free of the current legal regime, which many organisations believe is too legalistic and impractical. This goes beyond data protection laws and also includes the legal regimes for outsourcing, anti-money laundering and employment. Thus, it may be necessary to step back and create a new overarching framework that considers each of these elements holistically to create a friction-free framework.
- The UK Data Protection Act is difficult to understand, but the average business and "normal people" must be able to understand it. Perhaps "digitising" regulation is the way to overcome this problem as well as the excessive regulatory bureaucracy that currently exists. See The Future of Finance Report by the Bank of England for inspiration.
- Data protection, competition and consumer issues overlap. The UK must consider them all and bring them together into one holistic approach, where it makes sense.
- In trade negotiations, the ability to use data should not become a negotiating tool/bargaining chip and be traded away.
- The UK should create open data sets and develop appropriate data sharing frameworks so that multiple stakeholders can benefit from data.
- One of the biggest challenges is the global trend towards data localisation. Data localisation is at odds with current standards of access to information and with how the digital economy must work to function properly. It is ultimately detrimental to businesses, the economy and governments.

4. ***What tangible benefits can organisations see from increased global interoperability between international transfer frameworks?***

- Doing transfer risk assessments under SCC, developing BCR, obtaining certifications and implementing codes of conduct are resource-intensive endeavours that the UK must streamline. Organisations are spending significant time and resources on general GDPR compliance. Yet, they keep having to shift a significant portion of their attention and resources to international data transfers (especially after *Schrems II*), perhaps at the expense of implementing the rest of the GDPR effectively (which would often be more protective of individuals than can be accomplished through excessive focus on data transfers). Data flows are now one of the top compliance, commercial and strategic risks for companies, especially after the *Schrems II* decision and, potentially, in connection with Brexit.

- Given that the substantive legal regimes and standards that organisations implement often overlap significantly with other legal regimes globally, organisations should be able to leverage recognition, approval or certification under one system towards recognition, approval or certification under another system. Thus, all such systems/mechanisms should be designed to be as interoperable as possible from the outset—on substance, process and terminology. In addition, the UK should work with relevant international partners to build tools and mechanisms to (i) identify gaps between the substantive requirements of different transfer systems and (ii) mechanisms for organisations to bridge these gaps (such as by certifying to any necessary additional requirements that were not included in a certification an organisation already has). Companies often build a single data privacy management programme across their global entities and they wish to see some recognition and streamlining of data transfer requirements across the world. They want to use a single certification or approval programme to achieve a certification and approval in all countries.

5. ***Are there benefits (economic or otherwise) to UK involvement in international interoperability frameworks if the personal data that can be transferred under these frameworks is restricted?***

- There can be significant benefits for UK involvement in international frameworks. Where there are substantive differences between the UK's GDPR-based requirements and those in international frameworks, interoperability tools and gap-bridging mechanisms can be built (see above). The Article 29 Working Party once started that process between BCR and the APEC Cross-Border Privacy Rules (CBPR). That process was suspended pending completion of the GDPR and has not been revived.

- Any such streamlining and broadening of cross-border transfer options will have a positive economic impact. It will also improve continued availability of products and services we have come to depend upon and expect to function, and which frequently rely on global data flows.

- Also, because of its unique position and potential role as intermediary between the EU and the global community, the UK is well-placed to take a leadership role on global cross-border data flows and help demonstrate how effective global data flow governance can work.

- It should be a UK government priority to enable UK competitiveness in the modern digital economy and global Artificial Intelligence (AI) race by streamlining data transfer requirements

that allow data to flow freely but accountably to and from the UK. The more data is available to the UK, the more data will be available for sharing within the UK, and the more UK businesses can leverage that data for data-driven innovation and digital products and services.

- International research confirms the extraordinary economic value of data flows to countries' GDP and to large companies, SMEs, start-ups and individuals. The research also shows the negative impact of data localisation on GDP, inward investment and the cost of doing business. (See the recent OECD Report "A Roadmap for Cross Border Data Flows: Future Proofing Readiness and Cooperation in the New Data Economy".)

- Data can be a force for good and for economic growth. Restrictive data transfer rules can impede economic activity and interfere with the effective collaboration and use of data to combat COVID-19. Data protection has the tendency to lose sight of that. Data protection tools, including data transfer mechanisms, must be agile, flexible and fit for the 21st century digital economy and societies. The UK is well positioned to find the proper balance. The goal should be to enable responsible, accountable and trusted global data flows.

II. UNLOCKING HE POTENTIAL OF ALTERNATIVE DATA TRANSFER MECHANISMS

1. ***How can the UK encourage the innovative use of, and improve, the GDPR's alternative data transfer mechanisms including BCR, standard contractual clauses, codes of conduct and certifications?***

2. ***How can the UK build on the GDPR certification provisions and promote the use of codes of conduct and certifications as a data transfer mechanism (e.g. bi/multi-lateral agreements to enable BCR to BCR transfers, promoting interoperability between UK and EU certification schemes or non-EU schemes such as APEC Cross-Border Privacy Rules (CBPR))?***

- The UK can encourage the innovative use of, and improve, the GDPR's transfer mechanisms. For example, it should take an outcome-based approach by incentivising organisational accountability through which companies are more likely to reach the most protective outcomes (i.e. the ones that prevent possible harms to individuals). It should also build such mechanisms with global interoperability in mind, in order to facilitate both UK-EU transfers and transfers from the UK to any other region.

- Below are examples of how the UK can support and incentivise an outcome-based and accountability-based approach to international data transfers, as well as encourage the innovative use of data transfer mechanisms:

  (a) Streamline BCR:

  - Streamline the BCR approval process and make it more efficient (BCR have received a popularity boost post *Schrems II* and some organisations are now more actively thinking about using them).

  - Consider allowing enforceable self-certification of BCR (and for certifications; see discussion of certifications below). This would include a published list by the ICO and the ability to verify and enforce against false representations.

- Broaden the BCR to legitimise data transfers between non-affiliated organisations that have received approvals of their BCR—controllers, processors, sub-processors and undertakings engaged in joint economic activities, as per the GDPR.

(b) Give flexibility to SCC:

- Update SCC in light of the GDPR and *Schrems II* and allow organisations flexibility to adapt the SCC to their specific contexts.
- Allow uses of multi-party SCC for intra-group entities, multiple transfers between two or more entities, and multiple controllers and/or processors etc.
- Consider accountability as a principle in SCC, with the desired outcome spelled out, versus specifying clauses and precise wording, especially in the case of sub-contracting. In particular, avoid prescription for processor-to-processor clauses.
- Recognise that SCC are not needed to legitimise transfers of personal data from processors in the EU back to controllers outside the EU. Such transfers would be a continuation of previous operations involving cross-border transfers, which was already framed by an appropriate transfer mechanism.

(c) Update GDPR concepts:

- Recognise that a clear distinction between the concepts of processor and controller is outdated and does not comport with modern business realities (e.g. many organisations are both controller and processor in the same transaction). Simplify and streamline such concepts in the UK data regime and in updated SCCs.

(d) Unlock the potential of codes of conduct and certifications:

- Develop codes of conduct and certifications for cross-border data transfers and streamline the processes for obtaining a certification and participating in a code of conduct. They should include options to certify an entire accountable privacy management program (as opposed to only specific processing operations, products or applications) and should be able to connect to other programmatic codes and certifications globally (such as the CBPR), and/or that can map to global standards such as to relevant ISO standards.
- Consider enforceable self-certification *a la* Privacy Shield for some certifications (and also for BCR, see BCR discussion above) to streamline uptake by organisations. This could work if it is closely linked to the accountability principle and coupled with strong enforcement.
- Trade deals should recognise and support the use of codes of conduct and certifications as transfer mechanisms, similar to the United States-Mexico-Canada Agreement (USMCA) and the US-Japan Digital Trade Agreement.

- There is a link between accountability, BCR and certifications. Companies that have obtained BCR view it as a form of recognition/approval by DPAs of their privacy management programs. Accountable companies normally have a single global data privacy management programme through which they implement policies, procedures and controls that deliver compliance with

data protection laws across different countries and regions. This enables them to more easily meet the requirements for obtaining BCR and certifications across such jurisdictions, with due consideration to also adapting to any local requirements.

- 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. It should simultaneously encourage and enable UK businesses to participate in them and build effective interoperability tools that connect the CBPR to their counterpart UK/EU mechanisms, such as BCR, codes and certifications.
- Opening the CBPR to non-APEC countries is something that the APEC countries participating in the CBPR and PRP (US, Canada, Mexico, Japan, South Korea, Australia, Singapore, Philippines, Chinese Taipei (Taiwan)) 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 help drive more bridging between the CBPR and EU GDPR certifications, codes of conduct and BCR in the future. This earlier EU policy objective[1] unfortunately seems to have been abandoned by the EU Commission and EDPB (see above).
- The countries participating in the CBPR are also currently exploring participation by, or CBPR interoperability with, Brazil and India, both sizeable markets. Companies view inclusion of these and other significant global markets into a single transfer framework as a priority.
- Beyond participation in the CBPR, the UK should generally 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 can also pursue its role in the modernised Council of Europe Convention 108+ and become more of an influencer in that setting as well.
- Generally, the issue of how to govern global data flows should be addressed in global organisations, such as the G20, OECD, WTO, Council of Europe and Global Privacy Assembly, rather than letting the EU drive and dominate this issue.

3. Could organisations make use of other/additional safeguards to facilitate international data transfers? (E.g. security measures such as encryption, contractual measures such as GDPR Art. 28 checks on vendors, and committing to principles-based checks on overly broad or inappropriate government requests). How can the UK define such additional safeguards?

- The UK can encourage the use of additional accountability and risk-based safeguards and measures that could be considered and implemented. See the recent CIPL white paper "A Path

[1] Communication from the Commission to the European Parliament and the Council; Exchanging and Protecting Personal Data in a Globalised World, Brussels 10.1.2017, COM (2017) 7 final (emphasis added), available at http://ec.europa.eu/newsroom/document.cfm?doc_id=41157.

Forward for International Data Transfers under the GDPR after the CJEU *Schrems II* Decision"[2], which we have shared with DCMS.

- In addition, the UK should provide guidance to organisations on supplemental safeguards as well as on SCC and BCR. The DCMS and the ICO should collaborate on such guidance.

4. Are organisations currently making use of the Article 49 derogations as a legal basis for international transfers? If so, are there any specific challenges/barriers to this approach?

- In light of the *Schrems II* decision, reliance on the derogations may be appropriate and necessary for data flows that are essential or necessary to the delivery of contracted-for products or services and where other transfer mechanisms are no longer available. This is a topic that deserves priority attention in terms of the necessary legal and factual analyses involved. A potential challenge of this approach is the (potentially erroneous) view that use of the derogations must inherently be limited to minor and non-routine data transfers.
- Organisations do currently use derogations, but in a limited way, for specific transfers/contexts. Derogations are getting harder to use (the EDPB is pushing for an ever more narrow interpretation), and are time and resource-intensive. Companies prefer more holistic transfer mechanisms that do not require case-by-case assessments but deal with multiple transfers across the board. See more on the white paper mentioned in the question above and footnote 3.

III. BREXIT AND GDPR ADEQUACY

1. Are adequacy decisions under the GDPR helpful for organisations to transfer personal data from the EU to third countries and vice versa?

2. Do organisations also rely on alternative data transfer mechanisms even when the third country has been deemed adequate?

- There is no doubt that adequacy decisions are helpful to businesses. However, as a concept with broad utility, it is questionable given the difficulty of assessing a multiplicity of countries one by one, especially in an environment where laws and enforcement practices are ever evolving and dynamic.
- Overall, while it is always welcome to add another country to the "adequacy" list, the general approach on data flows should shift ideally from country-level adequacy to company-level accountability—which is what mechanisms like BCR, CBPR, codes of conduct and certifications can deliver. From an organisation's perspective, accountable data transfers should be about the accountability of the sending and receiving organisations and whether they provide the appropriate protections to the transferred personal data regardless of the country they are in. Some stakeholders therefore believe that, in the long run, the development of such mechanisms should be prioritised over country adequacy.

[2] Published on 25 September 2020. Available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_gdpr_transfers_post_schrems_ii__24_september_2020__2_.pdf>.

- Adequacy determinations are factual only on the surface; below the surface they are deeply political. The more the UK seeks to innovate, the greater the chance of losing adequacy. Such innovation, however, will not necessarily mean that the UK will be providing a lower level of protection to personal data. The question therefore is: how innovative does the UK want to be if it threatens a possible EU adequacy decision now or in the future? It is a dilemma and a fine line to tread for the UK. But the UK is also right in trying to be pragmatic.
- The prevailing industry view appears to be that adequacy should be the immediate goal for the UK and "innovation" with respect to alternative transfer mechanisms should come after adequacy has been secured.
- Companies rely on adequacy decisions and often just add the wording of the Article 28 of the GDPR in data transfer agreements to a recipient in the adequate country. Companies that use BCR are likely to apply their BCR in adequate countries as well.
- Finally, in light of *Schrems II*, there is legal uncertainty about the existing adequacy decisions. While companies are not currently prioritising the existing adequate countries for additional risk assessment steps, they realise that the existing decisions will have to be reviewed and are not likely to meet the "essential equivalence" test set forth in *Schrems II* (apart from Japan).

3. ***If the UK is not recognised as an adequate third country under the GDPR by the end of the Brexit transition period, how would this impact organisations? What measures should organisations put in place in order to maintain the free flow of data between the UK and EU as well as third countries? What are the biggest challenges and how can the UK support organisations overcome these challenges? What specific impacts and challenges would organisations face if they had to deal with multiple regimes simultaneously?***

- Loosing EU adequacy would have a significant impact on many organisations—global companies operating in the EU and UK, UK organisations operating in Europe, UK organisations delivering services to EU companies, as well as large companies and SMEs alike.
- Absent adequacy, the majority of data flows from the EU to the UK will have to rely on SCC – in their revised form and with supplementary measures implemented. Organisations exporting data from the EU will also have to conduct a transfer risk assessment in respect of the rule of law in the UK in relation to government access to data. This will include assessment of the proportionality and the existence of judicial remedies for individuals.
- The UK Government should publish an up-to-date digest and information on rules governing surveillance law and use of data in the UK, which should help reassure and assist companies in carrying out risk assessments.

4. ***If the UK is not recognised as an adequate third country, how could this impact other EU adequacy decisions?***

- It is hard to imagine other countries being found adequate if the UK isn't. The UK adequacy decision will be a test case for the continued viability of this approach. There is a tension between what is good for private sector organisations in the short and medium term—get UK adequacy ASAP—and what may be good in the long term—failing to get adequacy to demonstrate the inherent problem with the entire adequacy approach.

- As stated above, the EU Commission will have to re-examine all the current EU adequacy decisions in light of the *Schrems II* decision (apart from Japan perhaps). It is hard to see how many of the countries on the list can satisfy the high bar of "essential equivalency" of *Schrems II*. This is a big problem for the rest of the world.

5. How can the UK streamline the process for third country adequacy to the UK data protection rules post-Brexit?

- Essentially, this requires significant legal resources and expertise, coupled with developing a practical standard for adequacy that passes muster under the relevant UK legal standards (and EU expectations) without making adequacy findings impossible. This is a real risk, which is why the approach is fundamentally problematic.
- As mentioned above, the UK may want to consider sectoral adequacy (for data transfers within a particular sector), or processor adequacy (for transfers to processors in, for example, India).

IV. SCHREMS II

1. How can the UK government support organisations in undertaking risk assessments relating to third countries' data protection and national security and surveillance laws (e.g. assessment guidance and pre-assessment of countries to which UK organisations transfer the most data, pre-assessment of the UK for EU organisations wishing to transfer personal data to the UK)?

- The UK government and the Information Commissioners' Office (ICO) should work together on short-term solutions to *Schrems II*, such as guidance on international data transfers, developing UK-specific SCC, certifications and codes of conduct.
- The UK should provide to organisations as much information as possible about its own legal regime and the safeguards against disproportionate government access to data and surveillance for national security purposes. This should be based on the expectations of the CJEU and should provide a useful tool for companies in the EU that now have to conduct assessment of the UK's legal regime.
- The UK should also have or develop its own standard and template for assessing the adequacy of third countries, with due consideration as to where there is a discrepancy between what the laws of a third country say and what happens in practice. It should then provide a "popularised" version of it in the form of guidance to companies that now must undertake similar analyses of foreign countries in connection with using SCC. This guidance must be scalable to the realistic abilities of businesses, including SMEs and start-ups.
- The government should consider the impact of the *Schrems II* decision on its own adequacy findings, as well as on companies' assessments of third countries' legal regimes. The expectation is that the UK will have to follow *Schrems II* in its own approach to a significant extent, especially to achieve adequacy. But this would be problematic for all sorts of practical reasons mentioned above (and may also not be correct).

- The UK and other global governments should resolve the government access to data and surveillance issues on a separate track, without placing businesses in the middle.

2. What would be the impacts/benefits of a UK/US data transfer arrangement?

- A UK-US data transfer arrangement would be very beneficial from an industry perspective. Given that the UK was part of the EU-US Privacy Shield, it would make sense to create an extension or continuation of this arrangement for UK-US data flows. Any such UK-US Privacy Shield continuation should be developed with an eye to the parallel process of negotiating a new post-*Schrems II* EU-US Privacy Shield to maintain maximal consistency.
- From a US and global perspective, it is important not to cast or talk about such an arrangement in terms of a new bilateral UK-US arrangement. The US has publicly taken the position that, other than maintaining (or now fixing) the EU-US and Swiss-US Privacy Shield, it is not interested in pursuing further bilateral arrangements modelled on these Privacy Shields but would be pursuing other, multilateral cross-border transfer solutions (such as CBPR) for the rest of the world.
- A multilateral solution is ultimately a better approach and in the interest of everyone. Therefore, to the extent bilateral arrangements are pursued at all, it would be advisable to think of any UK-US bilateral transfer arrangement in terms of a continuation or extension of the UK-US' transfer practices under the former EU-US Privacy Shield so as to not increase further global demands for bespoke bilateral deals on this topic. This would make global data flows increasingly difficult to manage for companies. Companies ultimately require global, multilateral solutions to data flows rather than regional or bilateral solutions.
- Companies are aware of the need to strike a UK-US data trade agreement, as well as other agreements with the rest of the world (similar to the one UK just concluded with Japan). But they are also aware that the EU may be putting constraints on the UK in terms of adequacy. In particular, Japan is an interesting case study. The EU has granted Japan an adequacy determination, but has also compelled Japan to complement its Personal Data Protection Act provisions. The EU also did not allow onward transfers of EU data from Japan to third-countries based on the CBPR.

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; or Nathalie Laneret, nlaneret@huntonAK.com.