Lori Baker, Director of Data Protection, Dubai International Financial Centre Authority – Written Evidence (DAT0022)

1.What is your assessment of the existing adequacy arrangement underpinning data flows between the UK and the European Union?

It is an important mechanism for the free-flow of data from the UK-EU and vis-à-vis EU-UK. It provides certainty to businesses sharing data between both jurisdictions.

The arrangement had to continue post Brexit to avoid the skepticism it would raise regarding the overall EU adequacy system. If new Member States can simply join the EU and suddenly be deemed adequate with little evidence as to why, but an old Member State leaves and suddenly is no longer adequate even with EU retained law, it shows up the flaws in the adequacy mechanism in terms of how it is actually assessed (if it even is assessed).

a. What is your assessment of the value of the EU's adequacy decisions to UK organisations?

Although it provides certainty, the mechanism only supports the free-flow of data between the UK-EU. In the digital economy, data may flow to third countries due to the nature of the cloud and the structure of group entities. Therefore, it is important but not exclusive. Organisations would normally rely on Standard Contractual Clauses ("SCCs").

If the question is about adequacy decisions issued by the EU to other countries outside of the EU or UK, then it changes the response a bit. Given that only 14 other countries in nearly 30 years have been deemed adequate, the value really exists in terms of onward transfers of UK personal data from the EU to those countries. Some of them are valuable business partners, such as the US, South Korea, Israel, Australia and a few others, but generally speaking the SCCs have to be used for transfers to anywhere else, creating a papering exercise that effectively is a relatively redundant restatement of the law for which compliance already is necessary.

The EU adequacy regime has become so rigid as the apparent "only source of truth" that it risks stifling non-EU countries from issuing their own decisions. More on this below.

b. How are the General Data Protection Regulation and the Law Enforcement Directive working in practice? What extra costs do they impose on businesses?

They aren't working as well as they could. The fact that the question is framed in terms of costs to businesses rather than reinforcing individual data subjects' rights is a problem. The conversation around international transfers and privacy generally has lost sight of the real important questions, even with Max Schrems and NOYB continuously applying pressure to re-focus on the real issue – safety of my and your personal data. Furthermore, they could work better partly because there are so many carve outs in both laws (the LED more so that the GDPR) that leave policy and legislation to Member States, partly because of multiple layers of compliance that having both laws (and others) lends to confusion rather than clarity and harmonization and partly because this confusion means government authorities struggle to understand whether they are caught by the LED and if so, is it overreaching in terms of their remit as more administrative that enforcement driven.

The law enforcement directive has not been implemented in all Member States, and as it is a directive, it does not have to be implemented in the same way by all Member States.

A simple solution would be to implement something along the lines of Article 28 in the Data Protection Law, DIFC Law No 5 of 2020.

c. How would you assess the overall performance and effectiveness of the Information Commissioner's Office (ICO) as the UK's independent data regulator? Has its work been impacted by decisions on data adequacy?

No substantive comment or view on this.

The ICO is a leading regulator and its impact is seen globally.

2. What are the possible challenges to UK-EU data adequacy regime?

a. What factors could influence the next European Commission when deciding whether to renew its data adequacy decisions for the UK in June 2025?

Many respondents might say a change to the UK data protection laws as the obvious choice, but it seems to normally boil down to politics. Adequacy is about exactly that – or in more suitable terms from the GDPR, essential equivalence. If the UK changes its law for example, it will be unlikely to so fundamentally depart from essential equivalence with the EU such that adequacy will be revoked. If the change in the law or any other legislation or policy is not politically favorable in the EU's view, that will have the most impact.

b. What factors could the Court of Justice of the EU (CJEU) consider if the legality of the EU-UK adequacy decisions were challenged?

Looking at the previous Schrems I and Schrems II judgements by CJEU, the focus is on safeguards, human rights and judicial redress. However, I believe CJEU may also look at the following factors to determine whether the UK-EU adequacy decision is lawful:

- Is the UK DP regime 'essentially equivalent'
- Safeguards and oversight for surveillance activities?
- Is the UK still a member of the Council of Europe?
- Has the UK adopted and ratified Convention 108+?
- Does the European Court of Human Rights (ECHR) have jurisdiction?

In addition to the above, the CJEU should require the Commission to conduct assessments of the essential equivalence of EU Member States. This isn't done in practice, because of the legal and governance structure of the EU. However, as a general study and risk gap assessment, given that the EU Parliament for example declared that Hungary could no longer be considered a democracy, it would be an effective way to monitor internal affairs and whether the EU has real, sufficient adequacy amongst its own Member States.

d. How would you assess the possible impact of proposed UK rules on automated decision-making and the use of Artificial Intelligence on data adequacy?

It is essential to consider the effects of processing of personal data through autonomous and semi-autonomous systems, automations, etc. Considering there are still relatively few laws in assessed jurisdicitons, this might be a bit tricky, but both the UK and the EU have AI policies / laws in place and can review them in the next adequacy review.

Any adequacy decision going forward needs to include a review of whether privacy by design is embedded in generative AI systems that process personal data, partciulary high risk processing of such data, but not in the EU AI Act sense where it is prohibited full stop. Importantly, it needs to take a risk-based view and assess whether the laws permit such processing via certification or some other validation of the system, rather than outright banning it. Similar assessesments are already required for complex, advanced technology, but for truly smart, learning systems, there needs to be a view of whether a) the system provides sufficient notice to data subjects about how the spread and use of personal data is changing through ongoing deployment and use of the system, and b) if the laws of the jurisdiction require that the developer or deployer is able to provide evidence of safety from bias and other potential harms in the build of the system.

Please see Regulation 10

3. What implications, if any, would a no or disrupted UK-EU data adequacy scenario have?

The most likely practical outcome would be a contractual re-papering exercise where all (if not most) organisations will seek legal advice and look at the reliance on either a derogation under the GDPR or 'Standard Contractual Clauses' to faciliate the flow of data. However, as observed by the EU-US decision by the CJEU, there would likely be an urgent need to address the legal uncertainty by the EU Commission to facilitate and keep data flows open – and would most likely result in a new decision within 12-18 months.

The impact would largely be reputational, but not necessarily to the UK's disadvantage. Perhaps initially, yes, but there are many companies and privacy professionals looking for a new approach to data protection regulation and the UK may be the right country to provide it.

a. Do you have any concerns about the direction of travel of the UK Government's data policies as set out in the Data Protection and Digital Information Bill, and about the potential for greater divergence from EU data standards?

The UK should consider its sovereign interest. Divergence is not inherently negative. For example, focussing on balancing innovation with human rights is an area in which UK has always excelled. In order to be

more competitive, the UK should consider the needs of individuals and companies within the UK and take appropriate action in line with the needs of its citizens and companies. Compliance costs can restrict businesses whilst also complicating how individuals can exercise their right – it's important to take a position in the interest of data subjects and also businesses by removing procedural or unnecessary obstacles.

b. How high is the risk of the European Commission withdrawing its UK data adequacy decisions? What impact would that have and how prepared are businesses or the public sector for such a scenario?

There is a risk. I wouldn't consider it a 'High' risk because if you look at the last time any adequacy decisions were withdrawn, it was due to a decision by the CJEU. To date, the European Commission has not withdrawn an adequacy decision of its own volition – since that would indicate there may have been a failure by the Euopean Commission in the first one it issued.

c. What would be the implications for the continued operation of Part III of the TCA (law enforcement and judicial cooperation on criminal matters)?

No comment

Hopefully the EU Commission, if it intended to repeal adequacy for the UK, would do so with a plan for this in place. It's highly likely however that this sort of exchange of data is already caught by the existing provisions of UK and EU DP laws for data export, i.e., possibly via Article 46(3)(b), Article 48 or Article 49.

4. What can be learned from other countries' experience with the adequacy system and engagement with the European Commission's process?

From what I've observed, the European Commission process is unnecessarily lengthy, procedural, and far more focused on political relations than an objective analysis of a third country. There are over 130+ jurisdictions with a comprehensive data protection law, with a large number of members of the Global Privacy Assembly (GPA), the equivalent of the UN of Data Protection Authorities. However, the European Commission only deems approximately 14 countries outside of the EU adequate throughout the history of the European Directive 95/46 and the GDPR.

What can be learned is that the Euopean Commission approach may not stand the test of time as emerging markets and new blocs emerge which will look at a more multilateral mechanisms which respects each countries norms, laws and practices whilst ensuring a high standard which facilitates trade and investment.

a. What conclusions do you draw from the European Commission's recent adequacy review of 11 countries and territories?

The conclusion I draw is that it was expected that the European Commission will continue to 'grant' adequacy since removing adequacy would be an admission that its previous assessment may not have been in line with the Dir 95/46 and the GDPR. Also, to withdraw any of these decisions would be as disruptive and confusion as the CJEU Schrems decisions regarding the US. At least this way, the EU Commission has some control over the situation and can make a call that at least maintains some consistency.

However, as noted above, some of these jurisdictions should probably not have received a decision in the first place, particularly in view of blatant, on demand sharing of data with government authorities specifically to negatively impact individuals resident in certain countries, or simply the very liberal approach to sharing data with government authorities at all.

b. Are there examples of best practice which the UK could learn from in the way other countries approach their data transfer arrangements with the EU?

Are there other countries with data transfer arrangements "with the EU"? Such as ASEAN SCCs? These are all varities or offshoots of non-adequacy based mechanisms, not much to learn from that. The EU doesn't really do arrangements, do they?

Objectively, as in not in the specific context of dealing with EU transfer arrangements, but applied to all arrangements with other countries, the

DIFC Commissioner's Office has approached safeguards for lawful data export in a variety of ways, many of which have been shared with the Department of Science, Innovation and Technology. Please refer to its data export and sharing webpage for further information, particularly the non-legislative consultation materials on multilateral "adequacy" data sharing platform and regarding the Ethical Data Management Risk Index and supporting due diligence tool.

c. What are the implications for the UK's EU adequacy status if the UK grants its own adequacy decisions to other third countries currently not subject to EU adequacy?

There may be political ramifications, however my view from a practical perspective there would be limited to no impact. The UK is a pioneer when it comes to data protection and privacy safeguards. If in any case the EU Commission or the CJEU found the UK does not provide an adequate level of protection, the whole EU adequacy mechanism would need to be overhauled because a lot of other countries such as New Zealand, Argentina, Japan, Jersey, Guernsey et al would be most likely be unable to achieve the 'essential equivalence' standard.

Eighty-five (85) jurisdictions vest powers in either a data privacy regulator or government authority to designate other jurisdictions as having "adequate" data privacy standards, as per the IAPP report on adequacy capabilities. The EU has, as first mover, become the harbinger of adequacy decisions, but each and every one of these 85 jurisdictions have lawful rights to issue their own, and very well should, without worry or concern about what the EU might think about it. While a lot of transfers have to pass through the EU, there are a fair few that do not and additional decisions, a neural network between other jurisdictions, would ease compliance burdens with a more collaborative sense of oversight. Also it would make the matter of international transfers truly international, rather than indentured to the EU decisions.

DIFC has seen what it is like to approach a non-EU adequate jurisdiction that is reluctant, perhaps even fearful, of mutual recognition with DIFC due to "what the EU might do". This can't be the best approach, and the UK can be a leader in this very much needed approach. Ideally, the EU would be willing to work more globally and multilaterally – in actual practice, not only in intention.

d. If the UK joined the Global Cross Border Privacy Rules system, what impact if any could that have on the UK's EU adequacy status?

In my opinion, very little impact. What impact did it have on Japan, Canada, South Korea, and/or other Asian Pacific Countries? At most, it may potentially sour political relations. It is important to note that the UK's data protection history and practices are the most closely aligned with the EU model. If the UK for any reason is deemed 'no longer adequate' because it wishes to follow Canada and other 'adequate' members then the bar would be set impossibly high for the rest of the world and would ultimately impact the EU's ability to recognise third countries.

Received 6 September 2024