Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

21 December 2020

Comments by the Centre for Information Policy Leadership on the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Executive Summary

The European Data Protection Board (EDPB)'s recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (the Recommendations) should seek to achieve consistency, provide legal certainty and offer workable solutions to organisations that enable them to maintain international transfers **in line with the Court of Justice of the European Union (CJEU) "*Schrems II*" decision** (Decision or Court Decision). The EDPB should therefore properly balance the right to protection of personal data against other fundamental rights and interests, by taking into consideration the risk of business and social disruption. Indeed, after the Court Decision, organisations may be reticent to engage in activities that inherently depend on seamless global cross-border data flows, such as communication and networking platforms, e-commerce, international financial transactions, remote working and education, health care research, fraud and cyber threat prevention, travel-related booking and services, cloud services or outsourcing activities.

The Recommendations should clarify their **risk-based approach** in the context of international transfers, in order to better align (1) with the CJEU's mandate to look at the full context of a transfer and (2) with the GDPR's requirement to consider the risks, of varying likelihood and severity, for the rights and freedoms of individuals. The risk assessment requires a holistic approach, whereby no criterion by itself is decisive as to the outcome of the analysis. It should be based on empirical evidence, including previous history of government requests, which is an objective standard.

The Recommendations should also be **fully aligned with the General Data Protection Regulation (GDPR) and existing EDPB guidance**. Some of the current wording relating to the responsibilities of controllers and processors, or consent of individuals, should be reviewed. The EDPB should also enable reliance on Article 49 GDPR derogations and may want to reconsider its interpretation in light of the small number of Article 45 GDPR adequacy decisions. The relationship between the Recommendations and the EU Commission new standard contractual clauses for international transfers (SCCs) must be clarified and their implementation timelines should mirror one another. The Recommendations should acknowledge the huge compliance work required from all organisations (including public entities and SMEs) and set out the EDPB's work plan to assist organisations in their compliance efforts. **Data protection authorities (DPA) enforcement should be measured and proportionate** and based on a phased approach that the Recommendations should clarify.

The Recommendations should also better integrate the flexibility offered by **CJEU and European Court of Human Rights (ECHR) case law** regarding (1) the fact that national security activities authorise interferences with individuals' rights, and (2) that State authorities should be granted deference when deciding on the necessity and proportionality of restrictions to fundamental rights in the interest of national security. The Recommendations should refrain from mentioning any **specific country**. When referring to the United States (U.S.), the Recommendations should avoid suggesting that data transfers to the U.S. are largely prohibited and should take into account the limited scope of data covered by FISA 702 as well as the evolution of U.S. laws and practice on government surveillance.

CIPL welcomes the examples of **supplementary measures** and recommends that the EDPB provide a non-exhaustive and future-proof toolbox from which organisations can choose, considering what is most appropriate on the basis of their risk assessment. The Recommendations should not make any predetermination on the supplementary measures, which should be remain realistic and workable in practice. **Technical measures** should not have the adverse effect of impacting global security efforts. They should not be prescriptive and should refer to the type of threats organisations have to address. Depending on the circumstances, plain text access to data should be possible, decryption key management should be left to the choice of organisations, and hosting data in the EU should be considered as a supplementary measure. **Contractual measures** should be confirmed as possible standalone supplementary measures, depending on risk. It should not be expected that the parties will (1) enter into agreements requiring them to provide legal advice to each other, (2) systematically challenge government orders without regard to likelihood and severity of harms for individuals or (3) contractually agree to breach local law. The EDPB should also consider additional **organisational measures** such as certification schemes that provide for a uniform level of protection globally and enable organisations to leverage the safeguards they have already put in place.

Finally the EDPB should remove all **use cases** from the Recommendations, while setting-up an expert group to provide for meaningful co-design of use cases most commonly faced by organisations, or reconsider use cases 3, 6 and 7 as they are the most problematic ones, leaving organisations with no alternative solution to prohibitions on highly beneficial and routine data transfers.

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

21 December 2020

Comments by the Centre for Information Policy Leadership on the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

On 10 November 2020, the EDPB issued its Recommendations.[1] The EDPB invited public comments on this document by 21 December 2020. The Centre for Information Policy Leadership (CIPL)[2] welcomes the opportunity to submit the comments below as input for the Recommendations and thanks the EDPB for extending the consultation deadline to allow for more comprehensive feedback for the benefit of all stakeholders.

CIPL supports the effective protection of personal data and organisational accountability, including when data is transferred outside of the EU. We welcome the EDPB's initiative to provide organisations with recommendations to identify and adopt supplementary measures where required by the CJEU in its *Schrems II*" Decision.[3] (Court Decision or Decision). In particular, CIPL welcomes the EDPB's pragmatic approach of providing a six-step methodology, as well as a series of examples of supplementary measures and concrete case studies. CIPL further appreciates that many of the EDPB's Recommendations correspond to the spectrum of potential supplementary measures that CIPL highlighted in its recent white paper.[4]

CIPL strongly believes that the Recommendations are key not only to ensuring consistency in implementation of the Decision across the EU, but also to providing legal certainty and workable solutions

[1] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

[2] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and over 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. 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.

[3] The CJEU confirmed that SCCs are a valid mechanism for the transfer of personal data outside of the EU, while invalidating the EU Commission's adequacy decision on the EU-U.S. Privacy Shield, considering that U.S. law does not provide essentially equivalent protection under Article 45 GDPR for the fundamental right of data protection. It also held that in the absence of an adequacy decision by the EU Commission, organisations relying on SCCs for data transfers should assess the laws of the recipient country on a case-by-case basis, in order to verify the effectiveness of SCCs in ensuring compliance with EU data protection requirements. Where SCCs would not be fully effective, organisations need to consider additional safeguards and supplementary measures to the protection offered by the SCCs. The Court's judgment also requires DPAs to use their statutory powers to suspend or prohibit a transfer based on SCCs if, in light of all the circumstances of that transfer, the relevant DPA considers that SCCs cannot be complied with and the protection of the transferred data cannot be ensured by other means. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems; 16 July 2020; Case C-311/18.

[4] CIPL's White Paper on A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision.

for organisations faced with a very complex regulatory landscape. Consequently, it is of paramount importance that the Recommendations are fully aligned with the new SCCs for international transfers, as well as with the Court Decision, the GDPR and existing EDPB guidelines. In particular, CIPL emphasises the GDPR's acknowledgement that personal data flows "to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation" and that "technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries".[5] To be consistent with the GDPR mandate, the EDPB must seek proportionate and risk-based solutions enabling organisations to maintain business continuity and accountable data transfers for the benefit of the EU economy, society and individuals. This is even more important when Europe is seeking to re-establish economic growth in the years following the COVID-19 crisis.

Organisations of all sizes, sectors and geographies doing business in the EU are now tasked with assessing risks and devising and implementing measures to address the inherent tensions between the standards required by the GDPR - as interpreted by the Court Decision - and laws and practices globally in the field of law enforcement and surveillance. In doing so, organisations require pragmatic and balanced regulatory guidance that: (1) is protective of the fundamental right to data protection in relation to other fundamental rights and freedoms (including the right to conduct business[6]), (2) translates the Court Decision into practical steps for organisations, consistent with existing accountability mechanisms under the GDPR, (3) does not put in place insurmountable obstacles to transfers of personal data outside the EU where the risk and harms of governmental surveillance do not materialise and (4) does not force organisations to resolve conflicts with foreign laws themselves.

This constructive approach is necessary in light of the GDPR's requirement to balance the right to protection of personal data against other fundamental rights, in accordance with the principle of proportionality.[7] As a consequence, the EDPB should consider that transfers are essential to the economic growth and competitiveness of the European single market.[8] It will ensure that EU industry leaders, as well as SMEs and start-ups, continue to have access to cutting-edge and emerging technologies available in third countries. Such technologies enable them to communicate effectively with all their stakeholders, collaborate seamlessly, break down geographical barriers, thrive on the global scene and ultimately grow their business. Data transfers enable SMEs, in particular, to reduce the technology divide where they generally lack the tech savviness and expertise that large corporations possess. Reinforcing EU capacities in high-performance computing is also crucial to tackle current and future challenges from pandemics[9] to

[5] See Recitals 6 and 101 GDPR, clearly evidencing that the European legislator's intent was for personal data to be able to flow to non-EU countries and not to be kept primarily in the EU.
[6] See Article 16 of the EU Charter of fundamental rights.
[7] See Recital 4 GDPR.
[8] See the December 2nd letter sent by government ministers and senior officials from the Czech Republic, Denmark, Estonia, Ireland, Lithuania, Poland, Romania and Sweden stating that "Overly restricting data flows would hurt the international competitiveness of our manufacturers and service providers and hinder the development of new digital business in Europe. It would also be seen as justifying the protectionist policies of a number of third countries, despite the very negative impact these policies already have on European companies."
[9] Vaccines and treatments could have been developed at speed if developers had access to large volumes of electronic health data and to supercomputers that rapidly searched for medicines that could be repurposed for COVID-19 treatments.

climate change. At the same time, providing reasonable access to data is also key to help governments fight terrorism, organised crime and other global threats efficiently in the public interest.[10]

Organisations have been working hard to address the requirements of the Court Decision, including by assessing and revisiting current data transfer practices, replacing or reinforcing data transfer mechanisms, introducing new organisational and technical controls and strengthening existing policies. CIPL welcomes the recognition of organisational accountability and that DPAs will "pay due consideration to the actions exporters take to ensure that the data they transfer is afforded an essentially equivalent level of protection." CIPL believes, however, that the interpretation currently proposed in the Recommendations may, in some instances, go beyond the requirements of the Court Decision, often without added benefit for the protection of individuals.

Part I of this response sets forth CIPL's general comments on the Recommendations and **Part II** analyses the examples of supplementary measures and use cases. The **preliminary remarks** highlight the potentially significant consequences of issuing recommendations that go beyond what the GDPR contemplates and what the Court Decision requires.

Preliminary remarks on the risk of business and social disruption

Cross-border transfers of personal data are an integral part of the day-to-day operations of most organisations in Europe, as well as global organisations operating in Europe. Organisations in all sectors, including public sector bodies, routinely rely on the SCCs or Binding Corporate Rules (BCRs) to transfer data.[11] These transfers take many different shapes and forms, involving controllers, processors and sub-processors, many different types of data, different processing purposes, and different recipients in different locations. The Recommendations place onerous and expensive compliance obligations on organisations that will require substantial time to implement and maintain, without necessarily increasing the overall level of data protection.

First, the six-step roadmap requires a detailed review of every transfer, including an assessment of relevant local laws of the importer's country and their impact on the protection of personal data under EU law. This requires sophisticated multi-jurisdictional legal advice, which many organisations are not able to afford, and creates a risk of conflicting conclusions between organisations. The costs of acquiring and implementing the technical measures that the Recommendations seem to favour (see Part II) constitute an additional burden. In most cases, data are transferred to multiple countries, especially for micro-services focusing on singular processing activities in different locations, technical support, development operations and business operations. While governments and international organisations have the

[10] Intelligence and law enforcement authorities in the EU also request access to data held by organisations to fulfil their missions. The EU Council and the EU Commission have both recognised the importance of these objectives. See for instance the Joint statement by the EU home affairs Ministers on the recent terrorist attacks in Europe published on 13 November 2020.

[11] CIPL highlights that in the absence of other transfer tools under the GDPR that allow for regular data flows to multiple countries, organisations rely mostly on SCCs. Organisations may prefer SCCs over BCRs (that cover only intragroup operations with a long and costly approval process) and adequacy decisions (that cover only a few countries and that could be invalidated any time).

capacity to conduct detailed analyses and explanations as part of adequacy assessments, companies cannot realistically be expected to complete a highly detailed and sophisticated analysis for every transfer.

Second, given the scale of efforts required, most organisations, including SMEs, start-ups, charities and public entities, may consider immediate full compliance far too unrealistic and an unsurmountable hurdle. The imposition of these standards on SMEs in particular will create barriers to market entry, drive up costs unnecessarily and reduce the availability of customer choice in the market. These smaller organisations will also have to divert time and resources away from core GDPR compliance activities that may have a greater impact on individuals. A 2015 study actually found that companies would pay 30-60% more for their computing needs if localisation rules were adopted.[12]

Third, there is a risk that if non-essential obligations are imposed on EU organisations without tangible benefits for EU individuals, this may feed into anti-GDPR propaganda promoting the message that data protection law hinders EU's full engagement into the modern digital world.[13] It may be difficult for European organisations to achieve a "vibrant community of innovative and fast growing start-ups and small businesses" if they are not able to derive benefits from global data flows, or if they do not have access to the readily available, reasonably priced components that allow for the security of personal data and processing in line with GDPR requirements. These include, for instance, cloud services providing state of the art security, authentication tools, cyber monitoring services, customer engagement tools or HR management tools. Building such solutions in-house would be extremely costly, or even impossible, for most European organisations.

Fourth, there is a genuine concern that the Recommendations do not fully reflect the GDPR's risk-based approach and only provide for overly restrictive solutions that presume that all transfers, regardless of their nature, are "high-risk." This would amount to the Recommendations de facto advocating for data localisation in many instances. This would, in turn, trigger substantial economic and social disruption, in particular in the EU[14], and would be seen as incompatible with the GDPR objectives.

Finally, while a limited number of the services listed below, might, in principle, continue with some form of data localisation, such services likely will be degraded and/or would become economically prohibitive or non-viable without effective cross-border data flows. This comes at a time when the global COVID-19 crisis has accelerated digitalisation and has triggered a global reliance on digital tools and services at a magnitude never seen before. In addition, many of these services have enabled fighting of the virus at the national and international level, as well as continuation of business and social activities, education and a safe return to work.

More generally, it will be riskier for EU organisations to operate outside of the EU and to use commonplace and essential tools and services that inherently, and by default, presume and depend on seamless global cross-border data flows, such as:

---

[12] See study by Leviathan Security Group on Quantifying the cost of forced localization.

[13] See European Commission's strategy for 2019-2024.

[14] Many studies have outlined the significant negative economic impact of data localization policies that interfere with essential cross-border data flows. See, e.g., the recent OECD Report A Roadmap for Cross Border Data Flows: Future Proofing Readiness and Cooperation in the New Data Economy.

- **Social and professional networking platforms** - e.g., data flows enabling users to communicate, see or share posts across their global network of connections;

- **Communication platforms/tools** – e.g., employees sharing e-mails containing personal data – a copy of these e-mails will likely be resident on the recipients server;[15] the branch of a EU company in the U.S. requiring access to the agenda or customer file of its EU employees in order to communicate and share information with people globally;

- **Online cooperation and conferencing tools** - e.g., users registering for global online webinars/events; users recording conferences and other online meetings; employees using certain company tools or infrastructure, such as accessing company training programs;

- **Online forums, message boards and knowledge sharing sites** - e.g., users signing up to and sharing information depending on where the recipient's servers are located;

- **Online gaming** - e.g., users participating in online multiplayer gaming and gaming chatrooms;

- **Online learning** - e.g., users enrolling in distance online learning courses with international universities and educational institutions;

- **Online stores** – e.g., organisations connecting with customers and suppliers, providing information, taking and placing orders, and facilitating the delivery of products and services;

- **International financial transactions and investments** – e.g., users paying foreign merchants or transferring funds outside of their region;

- **Remote working** – e.g., working from home (which can be located anywhere in the world) has become the new normal under COVID-19 and is likely to remain so after the crisis;

- **Healthcare research** – e.g., global healthcare research relies on global data sets and international clinical medical trials are necessary to advance medicine and monitor the safety and effectiveness of existing medicine;

- **Research using online collaboration software**: e.g., EU-based universities and other research institutions engaging in collaborative research with institutions and organisations around the world;

[15] For example, if a German employee needs to send an email to a colleague in the U.S., this email will transit through internet infrastructure in the third country and end up in the system of the U.S. entity for that employee's review. In this case, both the German and U.S. affiliate process personal data and would be impacted by the Recommendations.

- **Fraud prevention and cyber security tools** - e.g., users benefiting from greater security because data is spread out over servers in different parts of the world to keep data secure, and personal data is shared for fraud detection purposes;

- **Round the clock customer service and technical support** - e.g., protecting users from service interruptions through distributed networks in other regions that enable back-up services; enhancing users' troubleshooting options by providing technical support services from outside the users' region;

- **Cloud service providers** – e.g., users storing data with cloud service providers that host data outside their region; cloud services hosted in the EU are often maintained from outside the EU;

- **Travel-related booking and services** – e.g., users booking vacations through domestic agents who send customer information to foreign hotels and airlines to secure bookings;

- **Health and wellness apps** – e.g., users using wearables connected with health and wellness apps to connect with other users, share health statistics and participate in fitness challenges;

- **Non-profit and humanitarian activities** – e.g., international NGOs and charities collaborating on cross-border initiatives on a daily basis to prepare the channels that enable international response, conducting of research in their areas and understanding of global trends;

- **Daily developments in technology and testing** – e.g., the growing diversity of data uses and emergence of new business models trigger more complex and dynamic relationships between organisations across different regions; and

- **Outsourcing of customer service activities** – e.g., companies outsourcing customer service functions throughout their global offices with "follow the sun" service. Outsourcing of EU HR, accounting, customer support, IT maintenance outside of the EU is commonplace, often to foreign professionals with unique skills.

I. General comments on the Recommendations

1. The Recommendations should clarify which transfers are excluded from their scope

Before the first step of the Recommendations' proposed roadmap titled "know your transfers," CIPL suggests the Recommendations clarify the types of transfers that are not covered by the Recommendations, namely:

- **Transfers to a data importer that is subject to the GDPR by virtue of Article 3(2) of the GDPR**: In this case, as the processing is already within the extraterritorial scope of the GDPR, the GDPR applies continuously from the point of collection of data from the data subject to the point of destination of the data and thereafter. This would align with the scope of the new SCCs.

- **Transfers that are initiated by the individual**: In many cases individuals themselves initiate transfers, such as by sending an e-mail, publishing a post, sharing a document, traveling to a third country or remotely accessing data stored by their provider in the EU. Those types of transfers are not attributable to the exporting service provider and are therefore not in scope of Chapter V of the GDPR and the Recommendations.

- **Transfers attributable to a third party**: In several instances, the Recommendations refer to actions by third parties in third countries by which they gain unauthorised access to EU personal data.[16] However, these actions should not automatically create obligations under Chapter V of the GDPR for the organisations, as they are often mere passive victims of a hacking by a third-party in a third country. Therefore, any resulting transfer cannot be considered an action attributable to the organisation responsible for the data processing operation that has been hacked.[17]

In Summary, CIPL suggests the Recommendations should clarify they do not apply:

- **To transfers to a data importer that is subject to the GDPR by virtue of Article 3.2;**
- **To transfers that are initiated by the individual; and**
- **To transfers that are attributable to a third party gaining unauthorised access to personal data.**

2. The Recommendations should clarify the risk-based approach in the international transfer context

CIPL is pleased to observe that several of the specific elements of the Recommendations inherently rely on the accountability principle and the GDPR's risk-based approach to compliance and data protection. However, in their next iteration, the Recommendations should be more explicit in acknowledging the role and function of the risk-based approach in assessing international transfers of data and in explaining how it applies in the context of Chapter V and to the supplementary measures contemplated by the Court Decision. Such clarification would also result in better alignment between the organisations' existing risk-assessment activities since May 2018, the Recommendations themselves and the CJEU's mandate to look at the full context of a transfer and to assess transfers on a case-by-case basis, in light of all the circumstances.[18] This means Recommendations should refer to and take into account the following:

- **Scope of the risk-based approach** – The GDPR risk-based approach covers all data processing activities as defined under Article 4(2) of the GDPR, and in an "end-to-end" manner. As such, it fully encompasses international data transfers that may be part of a broader processing activity.

[16] See Paragraphs 80, 85 or 131 of the Recommendations.
[17] Additionally, these types of scenarios will not even be "transfers" in many cases. In Footnote 14 of the Recommendations the EPDB makes reference to C-362/14 (Schrems I), paragraph 45 where a transfer is referred to as a "disclosure by transmission, dissemination or otherwise making available". However, controllers or processors storing data in their systems are not "disclosing" data to third parties that gain unauthorised access to such data.
[18] See paragraphs 121, 126, 134 and 146 of the Court Decision.

- **Criteria used for risk assessment** – Under Article 24 (1) and (2) of the GDPR, the technical and organisational measures designed to ensure compliance with the GDPR must be based on "the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons."[19] These criteria acknowledge different levels of risk depending on the nature of the data and the processing activity (including transfers) and enable organisations to tailor their compliance, control and mitigation measures to the actual severity and likelihood of risks and the specific context of a processing operation (including a transfer). For example, processing IP addresses or providing intra-group access to an employee staff directory (see use case 7) or business contact data would not trigger the same outcome as processing of health or communications data, as the potential risks to the rights and freedoms of individuals are different.

- **Holistic nature of the risk assessment** – By relying on a six-step approach, the Recommendations seem to suggest that risk assessments must be conducted according to specific chronological steps. However, organisations do not generally analyse risk criteria in isolation, one after the other, in a mechanical manner, but rather take a holistic approach, assessing different criteria together and against one another at the same time. Such methodology is broadly used for Data Protection Impact Assessments (DPIA) under the GDPR. This may result in a determination, for instance, that a country may have laws that are not adequate in the context of a specific high-risk processing activity, but appropriate for other processing activities.

- **Risk classification is inherently contextual and cannot be pre-determined** – An assessment of risk is always contextual. Although the notions of "high risk" and "low risk" for individuals have been established under GDPR as points of reference, the outcomes of risk assessments should not be pre-determined – otherwise, the overall goal of a risk assessment would be lost. Therefore, any risk assessment, including when an international transfer is involved, requires a concrete and nuanced analysis.

- **No criterion by itself is decisive to the outcome of the analysis** – The Recommendations suggest that once certain determinations have been made (i.e. existence of problematic foreign laws to which the importer may be subject), these are definitive and prevent any further and more refined risk analysis.[20] However, in this case, the organisation may also consider other criteria in analyzing risk,

[19] See Article 24 on the responsibility of the controller, Article 25 on data protection by design and by default, and Article 35 on data protection impact assessments. See Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01.

[20] FISA 702 is the only foreign law that is explicitly considered in the recommendations. The text box under Paragraph 44 states that if a data importer falls under the scope of FISA 702, the SCCs can only be relied on for such transfer if additional supplementary technical measures make access to transferred data impossible or ineffective. Moreover, the text box under Paragraph 76 further states that a data importer in scope of FISA 702 is under an obligation to turn over or grant access to personal data in their possession, custody or control. These conclusions capture by default all processing activities of organisations without any regard to other contextual factors such as the type of data concerned and potential relevance to authorities. It is not conceivable that the receipt of a law enforcement request covering one set of data can be taken to invalidate the relevance of SCCs for all other possible types of data, regardless of the circumstances relating to this data.

such as: (1) whether it has ever received any request to provide data under those laws; (2) the nature and sensitivity of the data; (3) whether the data may be of any relevance to and targeted by foreign authorities - many daily data transfers involving employees, visitors, business contacts, customers and services such as IT support, HR, marketing, finance, fulfilment, security and safety, are unlikely to be in scope, or (4) whether the data is otherwise protected under an obligation of professional secrecy of the recipient.[21]

- **Risk analysis based on the likelihood of risks materialising** – The Recommendations consider that organisations must adopt supplementary measures any time there is a theoretical possibility that data may be accessed in the context of a transfer, even if, in most cases, the transferred data is of no conceivable interest to third country authorities. This is inconsistent with Article 24 of the GDPR, which explicitly treats likelihood as a relevant criterion, and treats it as one based on objective considerations. Additionally, it is also incompatible with the recognition of the risk-based approach in other parts of the Recommendations. Indeed, because there is a theoretical possibility that data may be accessed almost any time a company uses the Internet to communicate with people outside the EU, or shares IT functionality with non-EU entities, this suggests that supplementary measures will be needed in almost every business transaction—regardless of the actual risk of access. Under the GDPR,[22] organisations may take into account objective criteria, which includes relevant criteria that go to the likelihood of a risk potentially materializing and potentially affecting the individual. When part of the processing takes place outside of the EU, organisations assess the risk in the same manner, by factoring into the assessment, for instance, the likelihood of access to data on the basis of the history of prior access requests or the relevance of the data to public authorities. If the likelihood of such risk materializing is low, organisations should not be required to adopt supplementary measures.

- **Risk analysis is based on empirical evidence** - Organisations do not transfer data for the purposes of providing personal data to governments but to conduct their business activities and best serve their customers. Governmental access requests are highly exceptional by nature when compared to the transfers conducted in the context of a relevant business activity. Therefore, the Recommendations should enable organisations to consider statistics on data access requests from foreign governments in view of the sheer volume of transfers carried out on a regular basis. This would avoid a situation where millions of users are prevented from using a service because the local authority submits a request for a negligible number of users.

- **Previous history of requests is an objective standard** – The Recommendations exclude the possibility of relying on "subjective factors such as the likelihood of public authorities' access to your data." However, the historical record of an organization's receipt of such access requests, from which a probability of future requests can be derived, is not a subjective factor, but rather an objective factor relevant to the severity and likelihood of the risk. Organisations will take different decisions

[21] See Theodore Christakis https://europeanlawblog.eu/2020/11/16/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-2/ "Even in a situation where the law of the foreign country clearly exempts some categories of data from the reach of government authorities (such as data covered by legal privilege or medical/professional secrecy) the EDPB considers that the data can only be transferred using strong encryption (cf. §85)."

[22] The GDPR relies on likelihood multiple times such as in Recitals 75, 76, 77, 88 and 90, as well as Articles 24 (1), 25 (1), 32 (1) and 34 (4).

depending on whether the likelihood of access to data by public authorities is low, high, or somewhere in-between. This approach is also in line with the new SCCs for international transfers that provide for an assessment of local laws, taking into account the specific circumstances of the transfer, which should include, inter alia, the assessment of "any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred."[23] Furthermore, the issue is not only whether this access is likely to occur, but also, to the extent it is available to the organisation, the purposes of this access (e.g., child safety, counter-terrorism, money-laundering fight, COVID-19 fight), as well as the seriousness of the risk for the concerned individuals. Organisations should be able to take into account the difference between providing data to governments based on where they are on the spectrum of being democratic or authoritarian and how the values they pursue align with those of the EU.

- **Evolving nature of risk assessment** – Organisations need to protect data in a continuous manner by implementing legal, technical and organisational measures ensuring continued effectiveness of data protection. In practice, this means that risk must be continuously monitored as evolving factors (such as changes in legislation and practices of the recipient country or availability of new privacy enhancing techniques) may change the risk calculus. A risk calculus that is subject to change over time, by definition, demands an ongoing risk-based and risk-sensitive response and does not allow application of a static, inflexible and definitive "high-risk" label to certain transfers. The Recommendations partly acknowledge this by stating that the right to data protection is active by nature and requires more than passive compliance. They should, however, more clearly recognise the continuous evolving nature of risk assessments.

- **Risk assessments built on existing processes** – CIPL agrees with the Recommendations' requirement for a case-by-case assessment. This should not, however, be interpreted as creating separate and isolated documentation requirements or as preventing risk assessments from being performed by type of transfers, processing activity, sector or data category. The Recommendations should encourage organisations to leverage the measures, tools and processes they have put in place to comply with existing GDPR requirements, such as records of processing activities, DPIAs or overall vendor due diligence.

Appendix 1 provides some relevant examples of processing risk assessments covering transfers outside of the EU.

In Summary, CIPL suggests the Recommendations should:

- **Confirm that the GDPR risk-based approach covers all data processing activities as defined under Article 4(2) GDPR, including international data transfers;**

- **Recognize the holistic nature of the risk assessment and that even in cases where problematic laws exist, organisations may also consider other relevant risk criteria;**

[23] See Recital 20 of the EU Commission draft Implementing Decision and clause 2(b)(i) of the new draft SCCs.

- **Acknowledge that if the likelihood and severity of risks materializing is low, organisations should not be required to adopt supplementary measures;**
- **Enable organisations to consider statistics on data access requests from foreign governments in view of the sheer volume of transfers carried out on a regular basis to assess risk;**
- **Include the possibility of relying on the historical record of an organization's receipt of government access requests as an objective factor relevant to the likelihood of risk;**
- **Acknowledge that organisations may take into account whether foreign governments' values align with those of the EU;**
- **Clearly acknowledge the evolving nature of risk assessments preventing any static, inflexible and definitive "high-risk" labels being attached to certain transfers; and**
- **Encourage organisations to leverage the work they have performed for GDPR compliance purposes to implement the Court Decision.**

3. The Recommendations should be aligned with the GDPR

CIPL recommends that the EDPB avoids departures from the GDPR's wording and interpretation and aligns with the new SCCs. This will avoid confusion when the GDPR is implemented by organisations, interpreted by DPAs or enforced by the courts.

First, the GDPR allocates different obligations, responsibilities and rights to controllers and processors. The Recommendations, however, appear to stretch the accountability obligations by imposing direct obligations on both the controller and the processor to demonstrate compliance to data subjects, the general public and DPAs.[24] While this may be relevant in practice, this is not explicitly required by the GDPR, existing EDPB guidelines or the Court Decision. The same comment applies to Paragraph 9 of the Recommendations requiring the exporter (defined as a controller or a processor) to inform data subjects of data transfers to third countries. This is excessive, as it is generally only the controller that has a relationship with, and direct duties towards, individuals. The Recommendations should not blur the lines of responsibility between controllers and processors, nor should they extend obligations to inform data subjects to processors that do not have a direct relationship with them.

Second, the Recommendations appear to take a disproportionate approach by failing to adequately balance the right to data protection against other fundamental rights and freedoms as required by Recital 4 of the GDPR, such as the right to life or right to access healthcare.[25] In line with Recital 4's recognition that the processing of personal data should be designed to serve mankind, the Recommendations should take into account more prominently their impact on individuals, acting as, for example, customers, employees, users or patients (and not only as data subjects). For instance, use case 4 in Paragraph 85

[24] See Paragraphs 3 and 7 of the Recommendations.
[25] See Articles 2 and 35 of the EU Charter of fundamental rights.

provides a scenario in which an individual needs to benefit from medical services that rely on an international transfer. This requires transit over infrastructure in the third country as well as cloud storage for which the Recommendations consider no measures to be adequate. The recipient in the non-EU country has to be able to read the data, so it needs to possess the decryption keys. Therefore, as no supplementary measures aligned with the EDPB's expectations are available, such transfers cannot proceed and would be unlawful. In this example, the consequences of not transferring the data could be tremendous to the patient, who, for instance, would not be able to benefit from imaging services.

Finally, the proposed supplementary measures must align with the GDPR and its interpretation by the EDPB. For instance, Paragraph 116 provides that data subjects could be empowered to exercise their rights and that data transmitted in plain text in the normal course of business may only be accessed with the consent of the data subject. However, the use case described occurs most commonly in every international company's everyday business operations, when employees routinely exchange electronic messages and access corporate resources. This could capture employee data processing that today is carried out under the grounds of "contractual necessity" or even "legitimate interests," where appropriate assessment has performed and documented with regard to the data in scope. Subjecting requests from government authorities to employees' consent contradicts the long-held position by the DPAs that consent can almost never be validly given in the employment context. [26]

In Summary, CIPL suggests the Recommendations should:

- **Be aligned with the GDPR, the EDPB guidelines and the new SCCs;**
- **Avoid blurring the lines of responsibility between controllers and processors;**
- **Not impose the obligations to inform data subjects on processors;**
- **Better balance the right to data protection against other fundamental rights; and**
- **Not rely on the consent of the data subject, taking into account existing EDPB guidelines.**

4. The Recommendations should respect derogations that are in line with the GDPR

The Recommendations suggest that only occasional and non-repetitive transfers may rely on one of the derogations provided for in Article 49 of the GDPR. CIPL submits that the Recommendations should be better aligned with Recital 111 of the GDPR and previous EDPB guidelines on derogations that differentiate between the various derogation use cases under Article 49. A firm statement that all derogations can only be applied to occasional and non-repetitive transfers is neither envisaged in the GDPR nor in previous EDPB guidelines on the matter. Restrictions which were not envisioned or intended

[26] This risks undermining the support that the EDPB and DPAs have given to classifying each of the six GDPR legal grounds for processing as being equal. See WP 249 - Opinion 2/2017 on data processing at work - Adopted on 8 June 2017 or CNIL guidelines, which supports legitimate interests and contractual necessity as appropriate alternatives for consent for a number of identified business management and commercial activities.

by EU legislators cannot be added via non-binding, soft law guidelines from the EDPB. Where EU legislators did intend to limit the use of derogations under Article 49, e.g., to occasional and non-repetitive transfers, when necessary for the purposes of compelling legitimate interests of the controller that are not overridden by the interests or rights and freedoms of the data subject,[27] the GDPR expressly provided for such restrictions with respect only to specific derogations.

More generally, the narrow approach of the Recommendations to Article 49 GDPR derogations leads to a lack of alternative legal transfer bases for organisations to avail themselves of when it comes to routine transfers. The Court Decision made clear that Article 49 should be capable of assisting where Article 45 and 46 GDPR cannot support transfers, something that the Recommendations have overlooked. The Recommendations should adopt a balanced and not overly restrictive interpretation, and take this opportunity to revisit its proposed interpretation of the Article 49 GDPR derogations in light of the importance the Court Decision attached to those derogations. This would enable organisations to continue to transfer data when necessary. Some of these derogations are not and cannot be considered "exceptional" for core services such as international communications or international money transfers. In this context, the EDPB needs to consider the combined impact of its narrow interpretation of the derogations, as well as the significantly small number of countries benefiting from Article 45 GDPR adequacy decisions.

Finally, CIPL recognises that derogations as a basis for data transfers may appear to offer less protection for individuals, given the lack of additional safeguards that are present in data transfer mechanisms such as SCCs and BCRs. However, we note that even when relying on a derogation in respect of a data transfer, the organisation still has to comply with the body of the GDPR and all of its principles, including data minimisation, purpose limitation, storage limitation, data quality, security, and the rights of individuals. These obligations and rights, the accountability and protection, do not stop because data is transferred to a third country, and are an integral part of the assessment of a data transfer and all its circumstances.

In Summary, CIPL suggests the Recommendations should:

- **Be aligned with Article 49 GDPR on derogations, in line with legislators' intent; and**
- **Review its interpretation and consider the small number of countries benefiting from Article 45 GDPR adequacy decisions.**

5. The Recommendations should make clear that enforcement by DPAs will be measured and proportionate

CIPL understands that the Court Decision takes immediate effect. However, due to the significant implications of the Recommendations, the EDPB should acknowledge that efforts undertaken by organisations to address the Court Decision require time and wide-ranging work, that goes beyond just turning off the data taps. These cannot be delivered immediately. This work includes legal and contractual

[27] See last paragraph of Article 49(1).

changes, requiring negotiations with third parties and covering, in some instance, hundreds to tens of thousands of contracts. It also involves implementing new business, go-to market strategies, as well as technologies, organizational solutions and changes affecting infrastructure, software and systems. In some circumstances, complete redesign of the architecture of a particular service is required. CIPL suggests that the Recommendations provide for a general element of reasonableness regarding how far organisations are expected to perform this work, especially in light of the risk-based approach of the GDPR and the reality of the changes required.

While CIPL welcomes the submission of the Recommendations for public consultation, we also note that they are applicable immediately following their initial publication and do not mirror the new SCCs' implementation timeline.[28] In addition, in their current form, the Recommendations provide that in the event that a DPA determines that an essentially equivalent level of protection cannot be ensured, the DPA should suspend or prohibit the transfers and impose a "corrective measure[s] (e.g. a fine)."[29] This focus on sanctions would force organisations, at best, to rush to quickly adapt their practices without addressing the risk carefully, and at worst would discourage organisations from undertaking substantive efforts in a short time-frame.[30] Any rushed plan may result in huge costs and additional administrative burdens, as well as impeding valuable uses of data for good. The Recommendations should instead be seen as an opportunity for the EDPB to provide its roadmap to assist organisations in their compliance efforts. For instance, as part of their tasks to promote the awareness of organisations, the EDPB and DPAs should assist organisations in implementing the Court Decision by maintaining and updating lists of important laws and regulations impacting transfers to certain countries, including guidelines on which legislation and non-statutory instruments may be relevant for specific sectors. This would enable organisations of all sizes to perform transfer risk assessments consistently and would decrease the level of legal uncertainty.

It is also important that the EDPB signal its own intentions for the timeline of corrective actions and their intensity depending on specific situations in, accordance with the principle of proportionality under Article 83(1) GDPR. The Recommendations should set out a consistent, transparent and risk-based enforcement framework, clarifying the process that DPAs will follow. Because of the novelty of the requirements resulting from the Court Decision for organisations charged with implementing them, it is essential that DPAs foster a reasonable and predictable procedure, so that accountable organisations will be recognised and compliance does not become a hazardous and unpredictable challenge, depending on which DPA is enforcing the ruling. To do so, CIPL recommends clarifying that under Article 58(2) of the GDPR, enforcing DPAs will adopt the following phased approach: (1) inform the data exporter of any concern regarding

[28] Note that the draft SCCs currently provide a transition period of 1 year, which is deemed insufficient by many organisations as indicated in CIPL Comments on Standard Contractual Clauses for Personal Data Transfers under the GDPR.

[29] See Paragraph 54 of the Recommendations.

[30] See Théodore Christakis https://europeanlawblog.eu/2020/11/17/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-3/ "The vast majority of companies will find it very difficult to implement such measures. These companies will have three choices: a) Stop some activities that involve international data transfers or localise data in Europe – a solution that will ensure full compliance with the EDPB requirements, but which could incur substantial costs and disruption. b) Do nothing and continue operating as usual – a solution that is good for business but that might be fully in breach of the CJEU/EDPB requirements. c) Try to supplement technical measures with contractual and organizational measures – despite the fact that the EDPB has expressed doubts about whether this might be sufficient."

compliance, (2) issue a warning, and enable accountable exporters to demonstrate their compliance actions in a constructive and trusted way, (3) in the event that no solution is found, issue a formal notice, (4) if the organisation does not have the capacity to comply, consider enforcement and corrective action, and (5) submit this decision to the Article 60 GDPR consistency mechanism in cases of cross-border processing, as defined by Article 4(23) of the GDPR. Finally, the mitigation factors, as well as calculations of the level of fines, should be set out transparently by the EDPB.

The fact that any organisation that uses an online service to process and transfer personal data—including email, videoconference and hosted applications—could face fines of up to 4% of its annual turnover, irrespective of whether public authorities in any third country actually or ever access the personal data in question, and whether this has caused any harm to the individuals, cannot be considered an acceptable implementation of the Court Decision. It would also fail to consider that Article 83(2)(k) of the GDPR provides that in determining the amount of an administrative fine, due regard shall be given to any other factor applicable to the circumstances of the case (in addition to those listed in Articles 83(2)(a) to (j) of the GDPR). This should include "the actions exporters take to ensure that the data they transfer is afforded an essentially equivalent level of protection"[31] but also duly consider that organisations have a passive role and may not be able to resist the acts of third country authorities, even when their safeguards are above market standards. In this context, the Recommendations should clarify that data transfers resulting from hacking of IT systems by a non-EU third party, gaining unauthorised access to EU personal data, should not result in any liability for the exporter under Chapter V GDPR (see Section I.1). This approach would encourage organisations to better address these issues thoughtfully and in good-faith, as companies organise their business and technical infrastructure to serve their business operations, not to serve the needs of national surveillance and law enforcement authorities.

In several instances, the Recommendations do not recognize the conflict of laws that often arise for organisations. They do not offer alternative options to a) self-incrimination to DPAs,[32] b) possible violation of applicable third country laws (that may go as far as contempt of court or obstruction of justice under that third country law) or c) the prospect of unnecessary and disproportionate business disruption. We still believe that these problematic conflict of law cases should remain exceptional and should not affect the vast majority of organisations and data transfers, provided the GDPR's risk-based approach is more explicitly integrated into the Recommendations (see Section I.2). It is key that DPAs tasked with enforcing Chapter V GDPR provisions accept that organisations are able to resolve the vast majority of these systemic conflicts in a pragmatic manner through the risk-based approach, so that only the most problematic cases for the protection of personal data are brought to the attention of DPAs.

Finally, the Recommendations and some of the use cases have the effect of forcing the application of EU law by encouraging organisations to purposefully implement roadblocks to government requests or demands for data, or to disregard a third country's rule of law and to contractually agree to do so.[33] This seems inappropriate, especially in case of lawful activities by authorities in those third countries conducted in the public interest (such as cyber-attack prevention, including in the EU). Conversely, it would indeed likely not be acceptable if a foreign law were similarly to encourage organisations to disregard the requirements of the EU law. In these cases of conflict, organisations should be given the

[31] See page 3 of the Recommendations.
[32] See Paragraphs 53 and 54 of the Recommendations.
[33] See Paragraphs 109 and 111 of the Recommendations.

right, consistent with principles of international conflicts of law, to request a review on international comity analysis[34], prior to a decision by a DPA, that would enable them to take into account the interests of both jurisdictions. DPAs should be in charge of examining both EU law and the laws of the recipient country which apply to that specific transfer, case-by-case, taking into account the fundamental rights and interests protected by each jurisdiction, prior to making a decision that suspends or prohibits data transfers.

In Summary, CIPL suggests the Recommendations should:

- **Acknowledge that organisations' compliance efforts require time and wide-ranging work that cannot happen immediately;**
- **Provide for a general element of reasonableness regarding the extent to which organisations are expected to perform this work;**
- **Describe the EDPB's roadmap to assist organisations in their compliance efforts;**
- **Commit to maintaining and updating lists of laws and regulations impacting transfers in certain countries;**
- **Take into account the new SCCs as supplementary measures and ensure implementation timelines mirror one another;**
- **Signal the EDPB's intentions for the timeline of corrective actions and their intensity depending on specific situations;**
- **Provide for a phased approach to enforcement by DPAs;**
- **Clarify that interception of data by foreign authorities overcoming appropriate security measures is not an act to which the exporter or importer has actively contributed; and**
- **Provide that in cases of a conflict of laws, organisations can request a review on international comity analysis prior to a decision by a DPA.**

6. The Recommendations should leverage the flexibility enabled by CJEU and ECHR case law

The Recommendations and the EDPB recommendations on European Essential Guarantees (EEG) (the EEG Recommendations) aim to set the stage, based on case law, for organisations to assess the existence of

[34] "Comity" is a legal principle in international law whereby a country should take into account other countries' important interests while conducting law and regulatory enforcement, in return for such other countries doing the same. The principle is based on the recognition that a particular enforcement activity by a country may affect important interests of the other country and may produce conflicts. See examples in the competition law sphere http://www.oecd.org/daf/competition/mou-inventory-provisions-on-negative-comity.pdf

the EEG in the third country's legislation. The organisation making the assessment ultimately bears the risk and duty to explain how it came to its conclusion, in particular with respect to what is considered necessary and proportionate. The Recommendations and EEG Recommendations, however, fail to consider that EU case law provides that national security agencies can be authorised under specific circumstances to interfere with individuals' rights. Organisations should be able to factor these key considerations into their risk assessments as well.

The CJEU ruling in La Quadrature du Net[35] recognised the importance of the objective of national security and acknowledged it could justify surveillance practices that result in interferences with individuals' rights, such as: (i) real-time collection of traffic and location data where there is a valid reason to suspect the person involved; (ii) non-real time collection of traffic and location data where the data might make an "effective contribution to combating terrorism"; (iii) general and indiscriminate processing of communications data for a limited period where there are "sufficiently solid grounds"; and (iv) general and indiscriminate processing of IP addresses and identification information, such as contact details. CIPL suggests that the same standard be applied to assess the laws and practices of EU countries and non-EU countries.

Some commentators[36] have highlighted that the restrictive interpretation by the EEG Recommendations of the case law of the ECHR would lead to the conclusion that no country, including EU countries, could pass the EEG Recommendations test. The EEG Recommendations consider, in particular, that State authorities should be granted deference when deciding on the necessity and proportionality of restrictions to fundamental rights in the interest of national security.[37] When coupled with the lack of clarity in the Recommendations on the risk-based approach (see I.2 above), this restrictive interpretation may lead to an automatic presumption of "non-adequacy" and insufficiency of supplementary measures. This could lead organisations to conclude that hardly any data transfer from EU to the rest of the world would be lawful. To avoid undermining the value of the EEG Recommendations, the EDPB should review its assessment for consistency with the full scope of CJEU and ECHR case law, including key factors which allow for national discretion.

In Summary, CIPL suggests the Recommendations should:

- **Include relevant EU case law confirming that national security permits interference with individuals' rights; and**
- **Include relevant ECHR case law, including key factors which allow for national discretion when deciding on the necessity and proportionality of restrictions to fundamental rights.**

[35] Judgment of the Court of 6 October 2020 - La Quadrature du Net and Others v Premier Ministre and Others - Joined Cases C-511/18, C-512/18 and C-520/18.
[36] See Théodore Christakis https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/.
[37] See ECHR Centrum för Rättvisa v. Sweden; Weber and Saravia V. Germany ; Big Brother Watch and Others v. the United Kingdom. Further, where the ECHR refers to surveillance measures prescribed by law, it applies a substantive interpretation that is not limited to the civil law tradition of acts of parliament and statutory provisions, but expressly covers unwritten law (Kruslin v. France; Chappell v. the United Kingdom).

7. <u>The Recommendations should take into account the limited scope of FISA 702 and the evolution of U.S. law and practice</u>

FISA 702 is the only foreign law that is explicitly considered in the Recommendations. The text box under Paragraph 44 of the Recommendations states that if a data importer (or sub-processor) falls under the scope of FISA 702, Article 46 transfer tools like the SCCs can only be relied on if additional supplementary technical measures make access to transferred data impossible or ineffective. Moreover, the text box under Paragraph 76 further states that a data importer in scope of FISA 702 is under an obligation to turn over or grant access to personal data in its possession, custody or control. The Recommendations seem to consider that all data importers fall under the scope of FISA 702[38] whereas FISA 702 requires consideration of the context of the data processing. The Recommendations should take into account not only the terminology used in the law ("foreign intelligence information"), but also the clarifications and assessment provided by the U.S. Government in the Schrems II White Paper[39] (U.S. White Paper) and the Privacy Civil Liberties Oversight Board (PCLOB) in their FISA 702 Oversight Report (Oversight Report).[40] As recognised in Paragraph 43 of the Recommendations, such reports are useful additional sources to assist organisations in completing their assessment. The U.S. White Paper states that "ordinary commercial data like employee, customer or sales records" that are transferred are not in scope of FISA 702 collection.

In addition, the Oversight Report states that there are two types of FISA 702 data acquisition - upstream and PRISM (downstream). Upstream applies only to 'internet backbone' providers and not any other organisations. In PRISM/downstream, the electronic communications service provider is required to provide communications sent to and from a communications selector (like an email address). This is also further acknowledged in the Court Decision (paragraph 61). Such communications data is a significantly more limited than all personal data processed by a covered data importer. For example, an electronic communication service may process customer-generated data like files or messages and their metadata, which are relevant under FISA 702. It may also process personal data strictly for billing purposes that is not of relevance under FISA, yet it would still be subject to the same approach under the Recommendations simply because data is processed by the provider in question. The Recommendations should therefore be clearer that FISA 702 covers specific types of data only and not all data processing activities of organisations.

The Recommendations further appear to fail to take into account recent changes in U.S. law and practices that would be helpful to organisations in performing their risk assessments, hence seemingly suggesting that data transfers to the U.S. are largely prohibited. We point out that this is not the conclusion of the Court Decision. For example, important changes and clarifications regarding the scope and operation of

[38] See footnote 49 of the Recommendations.

[39] Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II. This White Paper is intended to provide information on privacy protections under U.S. law and practice relating to government access to data for national security purposes to assist companies in performing their risk assessment when transferring personal data from the EU to the U.S. It includes developments on the role of the FISC in supervising whether individuals are properly targeted to acquire foreign intelligence information, redress available to individuals of any nationality for violations of FISA 702, privacy safeguards added since 2017 and clarification that transfers of personal data involve ordinary commercial information like employee, customer or sales records would not be the target of U.S. intelligence agencies.

[40] https://www.pclob.gov/Oversight.

FISA 702 requests have occurred. These include (i) the termination of "about" collection and (ii) the requirement under the FISA Amendments Reauthorization Act of 2017 that the government develop and submit for FISC (FISA Court) approval, as part of a FISA 702 certification package, or procedures regarding the conditions and limitations on querying information collected pursuant to FISA 702. In addition, declassified information has become available, demonstrating how the relevant safeguards and protections apply in practice, including those in relation to targeting determinations (and in particular, the requirement that the government memorialize a reasoned, written targeting determination for each individual target that is then subject to audit in a process supervised by the FISA Court) and querying procedures such as the information contained in the White Paper and explained in the Intelligence Community's 2018 Transparency Report.[41]

Finally, we question if singling out a particular country such as the U.S. in the Recommendations is really necessary and advisable, given the fact that the Court Decision impacts transfers of data from the EU to all third countries and that such transfers are a permanent feature of the modern digital economy. In any case, organisations need to conduct a risk assessment in respect of their processing activities and data transfers in a given context and to a particular third country, and not only in relation to the U.S.

In Summary, CIPL suggests the Recommendations should:

- **Consider the limited scope of FISA 702, which applies to data and not to organisations;**
- **Avoid suggesting that transfers to the U.S. are largely prohibited;**
- **Take into account recent U.S. law developments; and**
- **Remove country-specific examples given the global scope of the Recommendations and the global impact of the Court Decision on all data transfers.**

Part II. Comments on the Examples of supplementary measures and use cases

1. General comments

CIPL recommends that the EDPB address the following in its final Recommendations:

- **Provide a toolbox of supplementary measures** - Annex 2 of the Recommendations provides several use cases, but does not contain a clear and accessible toolkit of legal, technical or organisational supplementary measures for organisations to consider. Instead of proposing a one-size-fits-all approach, the Recommendations should propose a toolkit with a spectrum of potential safeguards and clarify that organisations should choose whatever safeguards they deem most appropriate based on their risk assessment and the context of a particular transfer. Such an approach would be aligned

[41] https://www.dni.gov/index.php/newsroom/press-releases/item/1867-odni-releases-annual-intelligence-community-transparency-report.

with the logic of Article 32 of the GDPR, which allows organisations to tailor their security measures based on various criteria. This would be of particular assistance to SMEs.

- **Do not show preference for (or rule out) specific types of measures** - The Recommendations state that organisational and contractual measures generally will not suffice to overcome access to personal data by public authorities, and that instead technical measures are required. However, as explained in Section I.2, any assessment of the relevance of supplementary measures vis-a-vis a particular risk must take all the elements of the data processing into account. Therefore, CIPL considers that the Recommendations should not prioritise certain types of measures over others, or flag some as being weak by default.[42] In line with the EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default,[43] the Recommendations should give organisations adequate discretion to decide which supplementary measures will ensure the protection of personal data and recognise organisations as being best positioned and equipped to adapt supplementary measures to the contextual risk of a transfer.

- **Clarify that supplementary measures have to be adapted to the risk** – Under the GDPR, mitigating measures should be adapted to tangible risks, based on the severity and likelihood of such risk, including in the context of international transfers. This means that the supplementary measures have to be scalable, too. They may well be unnecessary or minimal in the case of low severity and/or likelihood of harm to individuals, or conversely more important in cases of high risk. For example, depending on the specific context, organisations may choose different types of technical measures and combinations thereof, instead of solely relying on encryption with exporter-controlled keys. Some employee data could be protected by access management controls limited to a business function (such as HR), regardless of the location of the employee accessing the data, while in other scenarios access management with geolocation controls would be more suitable. In other words, in line with the GDPR's technology-neutral approach, what is appropriate will depend on the circumstances.

- **Provide for workable and "reasonable effort" measures in practice** – Some measures proposed may be impractical and go beyond state-of-the-art-practices.[44] For instance, in Paragraph 48, the Recommendations indicate that, to be sufficient, technical measures must impede all government access to data, including through encryption of data that is "flawlessly implemented" and resistant to cryptanalysis. It is unclear how a company can "flawlessly" implement encryption, or effectively prevent a foreign government, with all its resources and tools, from accessing data.[45] This would be predicated on knowledge and understanding of the capabilities of the public authorities or the types

[42] See for instance Paragraph 111 of the Recommendations, which considers that the contractual obligation on the importer to review the legality of orders to disclose data "will always offer a very limited additional protection."
[43] See Paragraph 8 - "The term measures can be understood in a broad sense as any method or means that a controller may employ in the processing. These measures must be appropriate, meaning that they must be suited to achieve the intended purpose, i.e. they must be fit to implement the data protection principles effectively by reducing the risks of infringing the rights and freedoms of data subjects. The requirement to appropriateness is thus closely related to the requirement of effectiveness."
[44] See for instance the recent state-of-the-art guidance adopted by the German institute and ENISA. See Paragraphs 3.2.4 for state-of-the-art encryption.
[45] The Recommendations would need to align with the definitions and controls outlined in international standards and industry-accepted encryption terms.

of data or access at their disposal, which is unlikely to be public information or information that companies would be able to reasonably anticipate, making these measures, by definition, unusable. Similarly, use case 2 provides that if data is pseudonymised, companies should take into account any information that the public authorities of the recipient country may possess to verify that the data cannot be attributed to an identified or identifiable natural person, even if cross-referenced with such information. This is an unrealistic expectation, especially when considering that national security and foreign intelligence activities generally operate with a high degree of secrecy. A better approach would be to allow organisations to use their reasonable efforts in implementing these technical solutions. Finally, the suggestion that data must always be encrypted at rest, with all encryption keys held solely in the EU (or other adequate jurisdiction), is practically impossible in all situations. Many uses of data, such as sending emails or texts, processing customer payments, or engaging in business collaborations, requires that data be available in a decrypted format. Otherwise, the data will be rendered unusable or encryption may generate functionality loss. In most instances, the transfer will lose its purpose.[46] Therefore, the practical application of the use case mentioned in the Recommendations is extremely limited and may undermine the relevance of the Recommendations overall.

- **Provide for proportionate measures** – The Recommendations should not go beyond requiring measures that are sufficient to address the risk in accordance with the principle of proportionality. As a consequence, they should acknowledge that organisational measures could, by themselves, be sufficient to narrow the access to data by public authorities. The Recommendations should also consider that if a solution does not primarily consist of the processing of personal data and is not subject to government access requests, it should not have to be completely redesigned to meet the Recommendations' standards.

- **Clarify that the Recommendations' list is not exhaustive** – Based on their risk assessments, organisations should be able to devise their own supplementary measures or mix of measures. For instance, in case of remote access for business purposes, access management and approval based on fine-grained controls or supervised access to personal data by an authorised European third party may be an effective supplementary measure. This would ensure that personal data is only processed to provide the service contracted for and that the actions performed do not transfer the data out of the EU. In addition, while encryption-in-transit and at-rest may not be sufficient by themselves where the importer possesses the keys, they could still be considered as technical measures of relevance when used in combination with other supplementary measures to protect basic personal data.

- **Make the supplementary measures future-proof** - The Recommendations should clarify that there may be a variety of ways encryption can be used effectively and that encryption and other technical measures can change over time. In addition, there may be further innovation in privacy-enhancing technologies, and quantum computing may also create quantum-safe cryptography techniques that

[46] See CIPL's White Paper on A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision "[…] there are instances where encryption is not suitable because it takes away the utility of the data and prevents necessary data processing activities by the recipient. This may result in preventing some product functionalities to be fully available, such as recording generally or integration of Data Loss Protection (DLP) solutions. It may also hinder the indexing of data or significantly impact user experience."

would make the Recommendations technically obsolete. The Recommendations should therefore provide flexibility to allow for the use of these developing technologies as potentially effective technical measures.

- **Take into account existing safeguards of organisations** – The Recommendations should consider that in most instances, data processing activities, including international transfers, are already substantially protected through the technical, organisational and contractual measures required by the GDPR, sector-specific regulations, relevant certifications (such as ISO) or other measures that organisations have implemented. Organisations will, in practice, build on these existing safeguards to determine whether additional measures may be required in light of the specific circumstances.

In Summary, CIPL suggests the Recommendations should:

- **Provide a toolbox of supplementary measures and clarify that organisations should choose whatever safeguard(s) they deem most appropriate based on their risk assessment;**
- **Not show preference for, rule out, or flag some measures as weak by default;**
- **Recognise that organisations are best positioned and equipped to adapt supplementary measures to the contextual risk of a transfer;**
- **Clarify that supplementary measures have to be adapted and proportionate to the risk;**
- **Provide for workable and reasonable measures in practice that do not require access to information that is not publicly available;**
- **Clarify that the Recommendations' list is not exhaustive and that organisations can devise their own supplementary measures or mix of measures;**
- **Make the supplementary measures future-proof by recognising that encryption and other technical measures can change over time; and**
- **Consider that organisations may already have existing safeguards and supplementary measures in place.**

2. Technical measures

While the Recommendations' main objective is to ensure the effective protection of personal data when transferred outside of the EU, the approach currently taken on technical measures may have the opposite effect of weakening the overall security of data in contravention of Article 32 of the GDPR. It is important to consider that fighting cybercrime requires processing of global training datasets that include personal data, such as the IP addresses of potential criminals. Security measures usually rely on exposure to attacks/vulnerabilities to "learn" how best to deal with them. As an example, a phishing attempt

originating in any single country in the world is useful information for an anti-spam model to identify and prevent similar phishing threats in other parts of the world. By restricting free flow of relevant data, the accuracy of machine learning models is undermined, which may lead to a proliferation of malicious activity at a time where accelerated digitisation triggers a growing number of cyberattacks.[47] Restricting the global free-flow of data is thus tantamount to unilateral disarmament in data security by the good side. In addition, transfer restrictions could also impact partnerships against cybercrime at large. For instance, this could prevent private CERTs[48] in the EU from exchanging information about cyber-attacks and threats, reducing the capabilities of EU public and private organisations to protect their systems against attacks. Altogether, this risks weakening cybersecurity globally, which impacts not only the security of personal data but the reliability of the EU digital economy at large.

In addition to the points already made above and to the analysis of the use cases, CIPL suggests that the Recommendations:[49]

- **Establish clear technical requirements/standards and outcomes rather than prescribe technical solutions** - Given the rapidly changing technological landscape, the Recommendations should rely on external market standards to ensure that organizations implement effective technical measures. Rather than prescribing the use of specific technical measures, the Recommendations should instead specify the type of threat organizations should be protected against. On this basis, organisations should be free to use any combination of controls to achieve the desired outcome (such as encryption, in combination with access controls and escorted access) as long as they are adapted to combatting the relevant threats.

- **Clarify that plain text access by the importer may be acceptable** - In line with the GDPR risk-based approach, the Recommendations should clarify that, depending on the circumstances, access to "plain text" (i.e. non-pseudonymised or non-encrypted data) may be acceptable. In addition, the access to plain text could be accompanied by mitigation measures - for example, where data access is intra-company and company security protections are consistent in both EU and non-EU locations, or where such access is temporary and any clear text data access is terminated (or the plain text data is destroyed) and certification is made that the access was for specific purposes and the data was not provided to third parties. Such flexibility is also key for the development of AI technologies where usability of data in plain text is required in the context of algorithmic training. CIPL underlines that the usability of homomorphic encryption remains limited and is not at a stage of development where it could enable full functionality and maintain the same level of relevance and performance.

- **Reconsider the requirement for the exporter to maintain its own decryption key** - While CIPL understands the rationale of requiring each exporter to maintain its own decryption key, we note that this may not always be feasible. Often service providers may have one solution supporting multiple

[47] ENISA specifically highlighted the increasing number of phishing campaigns and ransomware attacks on healthcare systems since the beginning of the COVID-19 crisis https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic

[48] CERTs stands for Computer Emergency Response Teams that handle and monitor cybersecurity incidents and store relevant data on these incidents.

[49] For more examples of technical measures and special considerations on encryption, see CIPL's White Paper on A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision at page 13.

clients, and the efforts necessary to implement a comprehensive change in practices will involve substantial time and resources. Providing the decryption key to each client could technically be very difficult. In addition, companies, and in particular SMEs, generally request that their service providers maintain the keys as they lack the resources and know-how to manage encryption keys - these are often much better managed and much more secure in the hands of a specialised technology provider. Further, lack of access to encryption keys will mean they can no longer rely on their provider's expertise to benefit from the latest features and more advanced security, which would ultimately result in a huge divide with the best of technology being accessible only to large businesses. In the end, encryption key management by the provider should not be ruled out per se. It should just be one of all the risk factors that should be assessed.[50]

- **Consider the hosting of data in the EU as a supplementary measure** - The determination that only technical measures such as pseudonymisation, anonymisation or "bring your own key encryption" can address the EEG gap, creates a de facto localisation requirement for a large category of data that have to be accessible in the clear for processing purposes. As mentioned earlier, CIPL believes that localisation of data in the EU is not a viable solution as data would still, in any case, potentially be accessible from outside the EU. However, to address specific situations where, for example, supplementary measures are not available, hosting data in the EU may be more appropriate than hosting it in non-adequate countries, even if some remote access in a third country remains possible or necessary for technical purposes. Even though the notion of "transfer" is broad, hosting data within the EU can be accompanied by other technical and organisational measures that address the concerns raised in the Court Decision as to the lack of transparency, judicial redress etc. Therefore, the Recommendations should acknowledge that EU hosting solutions can be assessed as a supplementary measure.

In Summary, CIPL suggests that the Recommendations should:

- **Not result in weakening of global security efforts;**
- **State clearly the type of threat organisations should protect against rather than prescribe the use of specific technical measures;**
- **Clarify that, depending on the circumstances, plain text access to data may be acceptable;**
- **Provide that the requirement for the exporter to maintain its own decryption key can be one of the risk factors assessed; and**
- **Acknowledge that hosting data in the EU can be considered as a supplementary measure.**

[50] Similarly, when privacy enhancing technologies such as pseudonymisation are used, what matters is not who holds the "additional data" or "where the additional data is held", but (1) whether it is effectively segregated from the pseudonymised data both technologically and organisationally, and (2) whether it is adequately protected and secured. These elements should also be factored in the risk assessment.

3. Contractual measures

In line with (1) the Court Decision that confirmed the validity of transfers based on SCCs even in the absence of technical measures, and (2) Recital 109 of the GDPR which states that controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement SCCs, contractual measures should be recognised as full-fledged supplementary measures, whether in a standalone manner or in connection with other technical or organisational measures, depending on the risk at hand.

Consistent with its previous comments, CIPL recommends that these supplementary contractual measures:

- **Be aligned with the EU Commission's new SCCs for international transfers**: Given that the Recommendations are intrinsically linked to the implementation of the new SCCs, the EDPB should clarify whether the new SCCs contain supplementary measures that meet the requirements of the Recommendations, and otherwise ensure consistency where possible. This means clarifying whether step 3 ("Assess the transfer tool") and step 4 ("Adopt supplementary measures") of the roadmap can actually be completed within the framework of step 2 ("Identify the transfer tool").

- **Be workable in practice**: For example, CIPL cautions against requiring importers to provide all information to exporters about the laws and regulations in the country of destination. This may amount to requiring the data importer to provide legal advice to the data exporter based on information that may not even be publicly available. This is contrary to current commercial practices and the reality of the relationship between controllers and processors. Processors absolutely refuse and are not in a position to provide legal advice to controllers, and controllers are also reluctant to rely on such advice. In any case, it is for the controller as exporter to conduct the transfer risk assessment and consider the law of the importing country in the context of a data transfer, not for a processor/importer to do so.

- **Be adaptable to the risk**: While it makes sense for the importer to review the legality of orders received by government authorities, the commitment to challenge the order should be predicated on whether there is a conflict with EU law, including in view of relevant case law, and based on the likelihood and severity of harms for individuals, not solely whether there are grounds to challenge the order under the laws of the third country.

- **Do not put the organisation in breach of local law**: The clause suggested in Paragraph 109 of the Recommendations requesting that the importer promptly secure or return the data, or if not feasible, delete or securely encrypt the data in the event of a government request, amounts to a contractual promise by the data importer to "destroy evidence" as soon as such evidence is requested by a third country authority, even if that request is perfectly lawful under local law. Doing this (and even just contractually committing to doing this) would immediately put the importer in breach of local law.

- **Not be overly bureaucratic**: Paragraph 114 provides that in the event of an order incompatible with EU law, the importer would have to notify the exporter and the DPA. However, given the commitment to challenge incompatible orders, it is not clear what additional benefit this notification would bring

and what actions the DPA would take on this basis. Similarly, the suggestion in Paragraph 118 to inform the data subject of a government access request may not be in his/her interest and would only serve to alarm data subjects, possibly without giving them meaningful recourse.

In summary, CIPL suggests the Recommendations should:

- **Be aligned with the new SCCs for international transfers and clarify their relationship;**
- **Provide that contractual measures may be used as stand-alone supplementary measures, depending on the risk at hand;**
- **Avoid imposing obligations on the parties to provide legal advice to each other;**
- **Clarify that contractual commitments to challenge government access requests should not be systematic, but be predicated on likelihood and severity of harm to individuals;**
- **Remove contractual commitments that would put the data importer in breach of local law; and**
- **Consider the benefits to the protection of personal data when imposing additional administrative requirements on organisations.**

4. **Organisational measures**

- **Consider additional measures**: CIPL welcomes the inclusion in the Recommendations of several organisational measures, including governance of access requests, publication of transparency reports, access control, timely DPO involvement and adoption of data security and privacy standards, as well as recognition under other data protection and/or data security certification schemes. In addition, CIPL recommends considering additional measures such as ISO certifications or other certification schemes that provide for a uniform level of protection globally and that can efficiently help global organisations assess and comply with relevant data privacy laws, particularly if the standard addresses specific issues such as local surveillance laws.

- **Remove the requirement that the team must be located in the EU**: From a practical perspective, CIPL believes that requiring that the teams tasked with assessing government access requests be entirely based in the EU may not be the most appropriate solution. These teams will likely need to engage with internal management that may be based outside the EU and may therefore be better placed, in some instances, through practical expertise to assess and, as the case may be, challenge the public authorities' requests. As long as the team has expertise, authority and resources to perform their tasks, it is irrelevant where they are physically located (and even more so in the times of global remote working post COVID-19).

In Summary, CIPL suggests the Recommendations should:

- **Consider additional organisational measures such as ISO certifications or other certification schemes that provide for a uniform level of protection globally; and**
- **Acknowledge that the teams tasked to assess government requests may also be better placed outside of the EU.**

5. Comments on most problematic use cases

CIPL suggests that the use cases be removed from the Recommendations for the time being. In parallel, CIPL recommends that the EDPB set up an expert group to provide for meaningful consultation, collaboration and co-design of use cases most commonly faced by organisations, with full fact patterns and consideration of different options. This would be more helpful and illustrative and enable organisations to make fit-for-purpose choices.

In the event that the EDPB decides to keep some of the use cases, CIPL requests reconsideration of the following use cases, as they are particularly problematic when read in isolation, without consideration of all the facts and without the application of the GDPR's risk-based approach:

- **Use case 3** on "**Encrypted data merely transiting third countries**" covers situations where an exporter wishes to transfer data to a country benefiting from an Article 45 GDPR adequacy decision, with the data routed via a third country. CIPL believes this use case should be reconsidered because (1) under the e-Commerce Directive, transit of data through a third country is not regarded as processing; (2) it is impossible for the exporter to know the exact route of the data (and therefore the third country implicated), because in reality internet traffic routing and management is defined automatically on the basis of load balancing; and (3) Point 7 seems to require every organisation to develop deep cryptographic expertise to understand the interception capabilities of other countries and design their applications to apply that expertise to a "flawless implementation". The information to perform such an analysis is not readily available, much less the technical expertise in such a highly specialised market. Expecting organisations to make determinations on the basis of such information is largely impossible and therefore disproportionate. CIPL therefore recommends removing the prescriptive provisions on encryption and replacing them with appropriate encryption approaches validated through risk assessment and schemes like, for example, ISO or the German Cloud Computing Compliance Controls Catalogue (C5).[51]

- **Use case 6** on "**Transfer to cloud service providers or other processors that require access to data in the clear**" covers the situation where an exporter uses a cloud service provider to have data processed according to its instructions in a third country. CIPL believes this use case must be revised because (1) the Recommendations pre-emptively conclude that there is a lack of effective technical measures to prevent access from infringing on data subject rights, whereas this assessment should be performed by the organisations as they have access to extensive information regarding the circumstances of the

[51] German Cloud Computing Compliance Controls Catalogue (C5).

transfer and their own systems and information (which the Recommendations overlook when making high-level assessments of such scenarios); (2) implied reference is made to "homomorphic encryption" as a possible solution even though that technology is far from being available for broad based commercial application, leaving organisations with no realistic alternative; (3) the use case does not address cases where the data can be seen in clear text by a machine that does the processing (and not by a human); and (4) the Recommendations do not appear to have considered a number of existing viable and proven security practices that include, for instance (a) the use of automated scripts to perform administrative action on customer data, whereby the scripts can perform restricted actions without any actual human access; (b) the use of cryptographic techniques with Cloud Hardware Security Modules whereby access is granted by the customer to a process that decrypts and acts on the customer data, but only under their control or (c) the use of split-key or dual-key encryption approaches whereby a key managed by the cloud provider and a key managed by the customer need to be simultaneously provided to enable processing of data.

- **Use case 7** on "**Remote access to data for business purposes**" covers the situation where an exporter makes data available to entities in a third country to be used for shared business purposes by the same group of undertakings. CIPL believes this use case must be reconsidered because (1) global companies need to make available (and access) EU personal data for all their core administration and business activities (e.g., HR, IT or customer management), with technical support often provided from outside the EU[52] and the Recommendations seem to suggest that no supplementary measures would be efficient without providing any alternatives (such as using a dedicated channel using VPN to access the data where it is stored); (2) the consequences of this use case could mean having an EU-originated website or digital service containing personal data prohibited from being accessed from third-countries; and (3) there seems to be a conflation between remote access and remote storage of data even though their respective risk levels are different. Access controls can be amended or terminated at any time by the EU organisation to render the data no longer accessible or available via remote access. The Recommendations should take this into account as well.

In Summary, CIPL suggests the Recommendations should:

- **Remove all use cases from the Recommendations for the time being;**
- **Set up an expert group to provide for meaningful co-design of use cases most commonly faced by organisations; and**
- **Reconsider the use cases 3, 6 and 7, should the EDPB decide to keep the use cases.**

[52] 24x7x365 availability and support is generally achieved by teams around the world via remote access. A requirement to use only providers who do not utilise support staff in third countries would result in a significant reduction in available service providers and, consequently, quality and quantity of services available to EU organisations.

Appendix 1 - Examples of risk assessments involving transfers outside of the EU

- **A medium sized tech company headquartered in the EU uses a number of off-the-shelf SaaS tools** to remain competitive. The company strives to have a strong GDPR compliance programme as it processes data of children but is also faced with budget restrictions. The company maintains a record of processing activities and has built a process to identify high-risk processing activities and complete DPIAs. If the organization uses about a hundred vendors for successfully running the business in a competitive manner, which requires transfers of user data outside of the EU, it must be enabled to build on its existing assessments and not start everything from scratch.

- **A global organisation uses standard communication tools**. As a result, business contact details of members of staff from the EU are accessed from Saudi Arabia where the organisation has offices. No other transfers of personal data for HR purposes are taking place from the EU to this country. As part of the overall assessment of all the circumstances of the transfer, it is possible to assess the relevance of this data to local authorities and the likelihood of data being requested.

- **The EU Commission transfers personal data of members of its Permanent Representation to Cuba**, either through the use of common systems or otherwise. If the personal data is only limited to the roles and professional contact details of such members of staff, it should be possible to assess the likelihood of the authorities requesting access to such data and the likelihood and severity of any potential harm to members of staff.

- **An EU-based controller has outsourced its procurement activities to a processor in India**. As part of the processing activities (engagement of the vendor), the teams in India collect personal data of representatives of the vendors and insert them into a tool that performs automated Anti-Money Laundering and Anti-Bribery and Corruption Checks, in accordance with UK and EU law requirements. As part of the assessment, it should be possible to assess the likelihood of the Indian public authorities requiring access to personal data of the EU representatives of such vendors.

- **An EU based controller has engaged a start-up in Brazil to develop a new app for direct engagement with its end customers**. The startup needs to have access to the data of the staff members of the EU based controller to deliver the service and may have access to the personal data of the users of the application (EU based customers) following its launch. The application only collects basic profile information such as e-mail, device identifiers, customer transactional history etc. As part of the assessment it should be possible to take into consideration the entry into force of the LGPD and the appointment of the Brazilian DPA, the Brazilian surveillance laws in Brazil, and likelihood and severity of risk in the event of access to EU staff and customer data.

***

CIPL is grateful for the opportunity to provide recommendations on the EDPB's Guidelines on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. If you would like to discuss these recommendations or require additional information, contact Bojana Bellamy, bbellamy@huntonAK.com, Markus Heyder, mheyder@huntonAK.com, or Nathalie Laneret, nlaneret@huntonAK.com.