Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision

Centre for Information Policy Leadership (CIPL)

September 2020

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

24 September 2020

A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision

On July 16th 2020, the Court of Justice of the European Union (CJEU) confirmed, in the case known as "*Schrems II*", that Standard Contractual Clauses (SCCs) are a valid mechanism for the transfer of personal data outside of the EU,[1] while invalidating the EU Commission's adequacy decision on the EU-US Privacy Shield. The CJEU considered that US law does not provide essentially equivalent protection for fundamental rights to data protection (due to lack of proportionate governmental access to data and the appropriate redress for the EU individuals in the US). The CJEU 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 supplemental measures to the protection offered by the SCCs, to ensure compliance with EU data protection requirements. The Court's judgment (hereinafter the "Judgment") also requires Data Protection Authorities ("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 DPA considers that SCCs cannot be complied with and the protection of the transferred data cannot be ensured by other means.

The Judgment substantially impacts organisations engaging in international data transfers under Chapter V of the GDPR (Transfer of Personal Data to Third Countries or International Organisations). Organisations are currently **working hard to implement** the requirements of the Judgment by assessing and revisiting current data transfer practices, switching or reinforcing data transfer mechanisms, introducing new organisational and technical controls and strengthening existing policies.

Organisations, and especially SMEs and start-ups, are also in great need of **clear and pragmatic guidelines** from the European Data Protection Board ("EDPB"), to ensure **consistency of the implementation** of the Judgement across the EU Member States and to provide **legal certainty.** Such guidelines should clarify the general expectations and how the Judgment will be interpreted consistently by DPAs. The guidelines should also contain a toolkit of possible measures that can be deployed by organisations based on context and risk, rather than prescribe strict technical or procedural requirements.

CIPL strongly believes that the EDPB guidelines must be informed by the reality of data transfers, global interconnected business processes and services, and best practices that companies are implementing to address the CJEU requirements. It is essential that the EDPB engages proactively with stakeholders and open these guidelines to public consultation during their development phase.

CIPL highlights that the Judgment impacts not only transfers to the US, but also all data **transfers from the EU to the rest of the world**. Organisations run the risk of being trapped by continuous conflicts of laws, a problem that they cannot solve by themselves. While practical and comprehensive EDPB guidance is needed in the short term to provide stability for organisations facing uncertainty, **wider and deeper constructive engagement** with organisations **and relevant EU and non-EU institutions is also essential going forward in order to build viable solutions for cross-border data flows.**

[1] Judgment of the Court of 16 July 2020 - Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems - Request for a preliminary ruling from the High Court (Ireland) - Case C-311/18; http://curia.europa.eu/juris/liste.jsf?num=C-311/18

CIPL has conducted discussions and a survey with CIPL member organisations regarding their data transfer practices. This Paper summarizes our observations and the findings of this survey concerning:

1. The GDPR mechanisms that organisations use or envisage using to transfer data outside of the EU in the post-*Schrems II* era;
2. The main factors organisations have identified to conduct risk assessments before data is transferred to non-adequate countries;
3. The supplementary measures that organisations are putting in place or envisage putting in place to protect transferred data; and
4. The organisational accountability frameworks and processes organisations use for responding to government data access requests.

This Paper also provides recommendations to the EDPB and the EU Commission for consideration when drafting guidance on supplemental measures for transferring data outside of the EU. These recommendations should also be considered when finalising the updated SCCs to reflect the GDPR's provisions and the CJEU's requirements in the Judgment.

CIPL highlights that this Paper does not necessarily reflect a single standard market practice of organisations. It is intended to provide a broad spectrum of current and possible practices that more sophisticated organisations we work with are currently implementing or are considering implementing in the future. The practices we list should **serve as a toolbox** from which organisations can pick and choose appropriate measures to address the consequences of the Judgment in light of their specific situation and the context of their data transfers. This toolbox may be also very useful to smaller organisations with more limited resources. The EDPB should ensure that their guidance and recommended measures are scalable for smaller organisations.

General findings of the CIPL survey:

- Consistent with the GDPR's risk-based approach, **organisations assess the risk** of transferring data outside of the EU in light of their specific situation, as well as the likelihood and severity of risks to individuals;

- Some organisations have been assessing data transfers outside of the EU as part of their **accountability obligation under the GDPR** (and other legal regimes) and already had mitigation measures in place before the Judgment;

- Some organisations view **accountability mechanisms such as BCRs, codes of conduct and certifications** as a solid framework for implementing possible supplemental measures;

- **Relocation of data/technology** or data localisation in the EU may not be a suitable, viable, or realistic strategy for most organisations, in particular when they rely on international communications or global support, which includes, but is not limited to, data-driven services, infrastructure management, fraud prevention, digital identity, electronic service providers or social media services providing real-time communication across the globe; and

- **Data localisation** in the EU also might not address concerns regarding government access, as the data may still be accessible through links with technology, networks, systems or entities in a third country. The mere fact that an organisation has establishments in multiple countries, including non-EU countries, makes it impossible to fully localise data.

I. GDPR MECHANISMS THAT ORGANISATIONS USE OR ENVISAGE USING TO TRANSFER DATA OUTSIDE OF THE EU IN THE POST-*SCHREMS II* ERA;

In the absence of an EU Commission adequacy decision (i.e., in the case of all but 12 countries, including the US for those organisations that relied on the Privacy Shield) organisations rely on several GDPR transfer mechanisms. As a direct consequence of the Judgment, organisations are reviewing their transfer mechanisms and may switch to new transfer mechanisms where necessary. They may also choose to combine different transfer mechanisms to address the current uncertainty, which is further fuelled by some isolated DPA guidance regarding the continuity of business transfers outside the EU.

1. Current Adequacy Decisions will be called into question – Article 45:

In prioritising the most critical tasks in the short term, the majority of organisations chose not to address their current data transfers to countries that are already subject to an adequacy decision. However, they recognise that all of these decisions will be called into question after the Judgment, once they are reviewed by the EU Commission. They fear that at least some of those countries will not pass the CJEU essential equivalency test. This creates legal uncertainty around those transfers in the medium term.

2. Standard Contractual Clauses (SCCs) – Article 46(2)(c):

The majority of organisations chose to rely on SCCs for their data transfers, subject to enhanced transfer risk assessments and additional safeguards as explained further in sections II and III of this Paper. Only a very small minority of organisations rely on ad-hoc, specific, DPA-approved contracts for their data transfers.

- Organisations use SCCs for **controller-to-controller transfers,** especially within the same group of companies**.** Organisations also use SCCs for **controller-to-processor transfers**, both within the same group of companies and in almost all other situations when using a third party service provider or providing access to data to service providers for processing /IT activities and services.

- As the definition of transfer is very broad, SCCs cover a **wide range of processing scenarios,** from physical storage outside the EU to mere access of data stored in the EU from a non-EU country.[2]

- For internal data processing activities, SCCs are often included in a **wider intra-group data transfer agreement,** serving as a comprehensive mechanism for a multitude of intra-group transfers (from IT tools and applications, e-mail, video conferencing, IT systems, cybersecurity and safety processes and tools, access to a global HR directory for employee management).

[2] These include, for example: 24/7 services which require different groups located across the world (including within the EU) to have access to and receive information from a single database; cloud services that rely on the free flow of data, even where the data are primarily stored in the EU, for example to update or replicate data for security purposes or to increase the speed of data transfers; financial and insurance services, including banks and payment platforms as well as other regulated services that rely on international transfers to comply with reporting requirements and that cannot be localised.

- SCCs are also regularly used for **transfers to (or access by) external third parties,** acting as processors on the instructions of the controller (such as, for example, IT maintenance, cloud computing or call centres), or as controllers (such as electronic communications or advertisers).

- Many of these transfers cover **essential services and business processes for all types of EU organisations,** regardless of size, activity and geographic outreach, as well as public entities and administrations. For example, all organisations extensively rely on cloud computing services for their daily commercial operations, including payment and accounting services.

- Companies continue to rely on the existing EU Commission SCC templates predating the GDPR (EU Commission Decision 2010/87/EC, Decision 2001/497/EC or Decision 2004/915/EC). They have been waiting for **updated versions of the SCCs that reflect the GDPR,** in order to avoid having to re-enter into SCCs twice in the short term.

- CIPL underlines that while signing SCCs can appear to be an easy and quick exercise on its face, it can be quite **disruptive for organisations** (both controllers and processors). It may involve updating thousands or tens of thousands of contracts. In addition, when SCCs are used for transfers between two separate organisations, they are often part of a broader contractual and commercial relationship. Having to re-engage in contractual discussions over SCCs may trigger the opening of wider commercial negotiations, preventing a "quick-fix" solution and introducing unwanted commercial complexities in the existing relationship. Prior experience following the Safe Harbor's invalidation in 2015 proved that the process could last up to two years for organisations with multiple business partners or vendors. In addition, at that time there was no uncertainty with regard to additional safeguards.

3. <u>Binding Corporate Rules (BCRs) – Articles 46(2)(c) and 47:</u>

The few CIPL member organisations that have received approval for their BCRs for controller and/or processor transfers continue to rely on them. They believe that the requirements of the BCRs (included in the EDPB guidances WP 256 and WP 257), coupled with transfer risk assessments and potential supplemental measures, provide a solid framework for meeting the requirements of the Judgment.

In order to have its BCRs approved, an organisation must demonstrate that it has implemented the following measures across the corporate group and all of its entities (several of these requirements may already work as possible supplemental measures to address the Judgment as described in sections III and IV of the Paper):

- **Right to lodge a complaint**: data subjects have the right to bring claims either in their state of residence, place of work or place of the infringement, giving individuals realistic redress options irrespective of where the alleged non-compliance occurred;

- **Increased Transparency**: there is a requirement for organisations to be transparent where third country legislation prevents them from complying with the GDPR as well as an obligation for any affiliated organisation bound by the BCRs to promptly inform the EU headquarters and the Data Protection Officer ("DPO") of this situation;

- **Commitment to Data Protection Principles** (including those listed in GDPR Art. 47(2)(d)): BCRs must provide that transfers of personal data by a member of the group signed up to the BCRs to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society, thereby compelling organisations to review each transfer or request for access to data in the context of the data protection principles under Article 5 of the GDPR;

- **Mechanisms for Accountability** under GDPR Art. 5(2); and

- **Commitments to inform DPAs about the third country government's requests for access to data** (including any legally binding request for disclosure of personal data by a law enforcement authority or state security body): if such legislation is likely to have a substantial adverse effect on the guarantees provided by the BCRs, it must be reported to the DPA with information on the data requested, the requesting body and the legal basis for the disclosure (unless prohibited to preserve the confidentiality of a law enforcement investigation). In this case an organisation must use its best efforts to waive the prohibition in order to communicate as much information as it can, as soon as possible, and be able to demonstrate that it did so. If it cannot notify the DPA, the organisation must provide information annually to the DPA on the number and type of requests it receives.

4. **Derogations (Article 49):**

- A few organisations rely on the necessity of the transfer for the **performance of the contract** derogation (Articles 49(1)(b) and (c)). This applies, for instance, to the multitude of HR processing operations necessary to fulfil the employment contract (e.g., timekeeping, payroll) in multinational organisations where its headquarters, central HR function and reporting lines are located outside of the EU. This derogation may also apply to global products and services whose delivery to an individual requires the involvement of different companies of the group.

- Some organisations rely on the necessity for important reasons of **public interest derogation** (Article 49(1)(d)), depending on the nature and purpose of the request received or the impact on fundamental rights and freedoms.

- Some organisations rely on the necessity to **defend rights and legal claims** derogation, (Article 49(1)(e)).

- Some organisations also rely on Article 49(1) when transfers are necessary for an **organisation's compelling legitimate interests** to operate (such as ensuring compliance with local law) and are not overridden by the interests or rights and freedoms of the data subject.

- To date, the majority of organisations do not systematically rely on derogations. Derogations are hard to use in practice and apply in specific contexts requiring a case-by-case analysis. Some organisations reserve the right to rely on derogations **in appropriate circumstances such** as for instance (i) where the data subject has given consent, e.g. where individuals participate in a voluntary stock investment program; (ii) in the context of the performance of a contract, e.g. where the organisation relocates employees to other countries, or (iii) to manage legal claims or regulatory interactions as needed.

- However, organisations do signal that they may be compelled to rely on derogations where appropriate and where, based on their transfer risk assessment, there are no other viable mechanisms they could use when conducting their necessary and critical data transfers. The CJEU has **specifically referred to the possibility of relying on derogations** and they are part of the GDPR's legal regime on international data transfers.

Unfortunately, organisations are unable to rely at this stage on **Codes of Conduct** (Article 46(2)(e)) or **Certifications** (Article 46(2)(f)) as data transfer mechanisms, as no guidance has been developed on how these tools can be used for international transfers[3] and none of these accountability mechanisms have yet been finalised. It is interesting to note, however, that some organisations consider that the external certification of their information and privacy management program (such as under the ISO standard), although not a valid transfer tool by itself under the GDPR, may constitute an additional safeguard (see section III below).

CIPL Recommendations:

- Acknowledge that switching to SCCs may be costly, resource intensive and may require extended time for organisations to comply with the Judgment;
- Confirm that the requirements of BCRs constitute a solid framework for supplemental measures to meet the requirements of the Judgment;
- Streamline the BCR review process and recommend an increase of DPAs' capacity to review and process BCR applications;
- Examine further how and in what circumstances derogations may be used by organisations to enable accountable, necessary and business critical data transfers and to make the most of the various transfer mechanisms provided by the GDPR and referred to by the CJEU;
- Develop guidance in consultation with organisations on supplementary and technology-neutral measures that would apply consistently to current and future GDPR data transfer tools; and
- Urgently work with stakeholders to define how codes of conduct and certifications can be used for international transfers. This will provide organisations with an additional accountable data transfer framework in which they can embed transfer risk assessments and supplemental measures.

II. THE MAIN FACTORS ORGANISATIONS HAVE IDENTIFIED TO CONDUCT RISK ASSESSMENTS BEFORE DATA IS TRANSFERRED TO NON-ADEQUATE COUNTRIES

To comply with the Judgment when there is no EU Commission adequacy decision with respect to the recipient country, organisations have to **assess the third country's legal system** in light of the Judgment's requirements, as well as the context of their data transfers. Many organisations have

[3] When used as international transfer tools, certifications and codes of conduct must be coupled with "*binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights*". It is necessary to analyse this requirement in light of the Judgment to ensure that a uniform and similar test is applied to all transfers tools.

already started doing this and are reviewing and adapting their existing processes. However, this is a laborious and expensive process, requiring skills, knowledge of third countries' laws (not only data protection laws, but also national security laws and practices) and access to external counsel that only the largest and most sophisticated organisations with strong legal teams and resources may have. There is a real fear that the vast majority of organisations in the EU and many controllers using third party processors, or separate or joint controllers, outside the EU will simply not be able to conduct this type of deep and continuous legal analysis of the legal frameworks in third countries as laws and practices change. There is also a concern that different organisations, legal counsels and DPAs may come to different conclusions with respect to a third country rule of law, which increases legal uncertainty and confusion in the digital ecosystem. To address this, CIPL calls for the creation of a single database of risks assessments across countries at the EU level, so that transfers are assessed in a consistent way. Such a database should be available on the EU Commission and EDPB websites.

The **data transfer risk assessment** is a key step in identifying potential risks associated with an organisation's data transfers and identifying mitigating measures commensurate with those risks. It is important that any regulatory guidance recognises the importance of these risk assessments in light of the risk-based approach enshrined in the GDPR. Consistent with the EDPB guidelines on DPIAs and high risk processing (WP 248), transfers to third countries should not automatically and *per se* be seen as constituting high risk processing under GDPR. It should instead be determined whether such transfers could result in a high likelihood and severity of risk of harm, for example due to governmental access to that data.

Organisations may choose to perform these assessments on a case-by-case basis, or per type of processing, business line, recipient or country as appropriate, depending on their structure and types of processing. They may also include them in their broader risk assessments on processing operations as part of their GDPR accountability obligations. The data transfer risk assessment can also be part of the preliminary risk triage that organisations perform to identify whether or not they fall under the obligation to perform a full-blown DPIA. Depending on the outcome of this preliminary analysis, organisations should remain free to decide whether to include this transfer impact assessment as part of the DPIA if one needs to be performed, or to establish a separate process specifically for the transfer itself. CIPL emphasises that the guidance should focus more on the objectives and outcomes of the risk assessment than on precisely how to conduct such a risk assessment. For the sake of efficiency, it is important that organisations can rely on their existing processes to identify and apply the necessary safeguards and mitigation measures where they are most relevant.

It will also be important to delineate the responsibilities of the data exporter and the data importer in relation to these assessments, as in some instances only one of them has access to the information needed to perform such assessments.

CIPL findings show that when performing these transfer risk assessments, organisations take into account the following factors pertaining to the data transfer itself (1) as well as factors relating to the laws of the recipient country and their application in practice (2):

1. **<u>Risk factors related to the transferred data:</u>**

   - **Nature of the data** being transferred (e.g. name, email address, employee data, client data); special categories of data as per Article 9 GDPR; sensitivity of the data such as metadata, localisation data, financial data;

   - **Nature of the data processing subject to transfer** (HR management purposes, clinical trial, fraud prevention, advertising etc.);

- **Categories of data subjects and the impact of the processing and transfer on them**, including severity and likelihood of harm if data is accessed by unauthorised third parties;

- **Likelihood of government access to certain types of data** (both from intelligence and other law enforcement authorities such as securities, anti-trust, anti-bribery, safety, pharmacovigilance etc.) and whether the data that is subject to the transfer is within the scope of intelligence and law enforcement activities;

- **Volume of data** transferred, including **number of data subjects** covered;

- Purpose of the data transfer and, if applicable, link to a **public interest recognized in the EU** in case of government access;

- **Volume of data potentially impacted relative** to the overall volume of data transferred;

- **Organisations' business model, and the business sector** in which the transfer takes place (B2B or B2C, Adtech, etc.);

- **Nature of the transfer** such as intra-group transfers or transfers to external third parties, controller-to-controller, joint controller, controller-to-processor or processor-to-processor transfers;

- **Duration and frequency of the transfer** - limited in time, ongoing transfer or access to data;[4]

- **Technical controls and organisational measures** in place or possible safeguards to protect the data (see Section III of the Paper);

- **Type of data recipient** (e.g. affiliate, partner, professional advisor, cloud service provider or other service provider);

- **Number, type and location of processors and sub-processors** involved in the transfer (including possible onward transfers) and **assessment of** processors/sub-processors including their organisational policies and history of disclosing data to a government entity;

- Existence of a **DPO or Chief Privacy Officer** within the data importer's organisation; and

- Data importer's membership or public support to organisations **advocating for the defense of human rights** (e.g., Global Network Initiative).

2. **<u>Risk factors related to the recipient country's national laws and legal practices:</u>**

- Legal framework or applicable privacy and security standards in the country of **destination offering the same or a similar level of data protection as the transferring entity's country.** This may include whether the country has adhered to international agreements

[4] In certain scenarios, structural transfers are more likely to be better protected for commercial and reputational reasons.

on data protection and cybersecurity (e.g., OECD Guidelines on Data Protection, Convention 108, Budapest Convention on Cybercrime, UN Charter of Human Rights, Madrid Resolution: International Standard on the Protection of Personal Data and Privacy, etc.);

- Availability of an **effective and independent recourse mechanism for individuals** (including EU individuals) to **enforce their rights** under the law of the country of destination;

- **Laws that may impact the protection** of transferred personal data such as those relating to national security, surveillance, and law enforcement, in comparison with the surveillance laws and practices of the country of the EU data exporter (as provided for instance by the European Agency for Fundamental Rights);

- Availability of **legal means for organisations to challenge** government access requests;

- **History and likelihood of government access requests in the specific context of the transfer**: whether the type of data at issue has typically been sought by government entities under local law, historical data on past requests, and the likelihood of such requests in the future, either generally or specifically as it relates to particular data; and

- **General human rights ratings of the country** of both the data importer and the data exporter regarding democratic practices and individuals' access to political rights and civil liberties (by NGOs such as Human Rights Watch).

CIPL Recommendations:

- Do not qualify transfers outside of the EU as high-risk processing per se;
- Acknowledge that organisations are conducting risk assessments as part as their GDPR accountability obligations;
- Focus on the objective of transfer risk assessments rather than on how to conduct such risk assessments;
- Provide flexibility to organisations to conduct transfer risk assessments as part of their existing DPIA or other due diligence processes;
- Acknowledge the different roles of data exporter and data importer in performing risk assessments; and
- Create a database of risks assessments across countries at the EU level so that transfers are assessed in a consistent way and all size and types of organisations have access to relevant information.

III. TOOLKIT OF POSSIBLE SUPPLEMENTARY MEASURES ORGANISATIONS CAN PUT IN PLACE TO PROTECT TRANSFERRED DATA

Organisations are currently reviewing existing processes and/or are putting in place a series of supplementary measures to mitigate risks when data is transferred to a non-adequate country. These supplementary measures are a combination of legal, organisational and technical measures. Consistent with the risk-based approach and Articles 24 and 32 of the GDPR, these measures have to be calibrated on a case-by-case basis depending on the severity and likelihood of risk of harm to individuals. The mitigating impact of each of these measures may differ depending on the risk being addressed. **Therefore, not all of these measures should be required or considered appropriate in every instance and for all organisations**. Several of these measures have already been or are being implemented by organisations as part of their accountability measures under the GDPR.

Based on its research and survey results, CIPL has identified the following **toolkit of possible measures for organisations to consider and choose from**:

1. **Legal measures**

- **Implementing additional contractual provisions and controls in controller to processor SCCs** to maintain the privacy and information security of the data: (i) Data Protection Addendums including GDPR Article 28 due diligence requirements; (ii) committing to a principles-based approach or an additional internal process on the checks carried out on overly-broad or inappropriate government requests and committing to appropriately narrowing down such request, and challenging requests which are not necessary and proportionate; (iii) liability and additional obligations (i.e. notice obligations, return or deletion of data and termination of the contract); and (iv) increased transparency on government access requests;[5]

- **Requiring additional accountability from the recipient** with respect to government access to data and setting up an **oversight mechanism** between the controller and processor(s), including: (i) processor reporting obligations to controller (subject to appropriate exemptions); (ii) quality assurance measures; and (iii) operational compliance measures;

- **Providing enhanced individual rights** vis-a-vis the organisation (e.g. informing individuals about the requests where legally possible, ad hoc redress rights mechanisms through mediation, or other similar mechanism); and

- **Commitment by organisations to challenge inappropriate government requests and to suggest that mutual legal assistance mechanisms be invoked** (in particular in situations where a disclosure in the recipient country would put the organisation in potential breach of applicable data protection law in another country that has jurisdiction or authority over the data).

2. **Organisational measures**

- **Risk assessments** to identify risks and appropriate mitigation measures – See Sections I and IV of the Paper;

[5] When suppliers do not include these additional contractual safeguards proactively, it may be challenging for smaller client organisations to force additional contract clauses or accountability measures on such suppliers.

- **Data minimisation**: transferring specific data only and not an entire database where the nature of the service so permits; limit transfer to or access from a third country to what is necessary to provide the service in a controller-to-processor scenario or to satisfy the legal basis on which the transfer relies on a controller-to controller basis;[6]

- **Obtaining privacy and data security certifications or adherence to a code of conduct** to demonstrate data minimisation and organisational security measures limiting the pool of data available for access;

- **Robust legal and operational policies** for government access requests governing: (i) the disclosure and provision of data pursuant to government surveillance, law enforcement and other legal requests; (ii) emergency disclosure policies; (iii) notification and transparency; (iv) user access policies; (v) internal access limitations and definition of roles and privileges; (vi) data retention and deletion protocols; (vi) legal challenge against unlawful or overbroad data requests where appropriate; (v) internal protocols and escalations for decision-making, and appointment of roles solely responsible for dealing with government requests for data;

- **Existing comprehensive Privacy Information Management System** that can also be certified by independent third parties (e.g. ISO 27701 for privacy or ISO 27018 for cloud computing). These certification standards generally include stringent controls on data disclosure;

- **Certification to the Privacy Shield** (not as an adequacy measure but to demonstrate the organisation's commitment to upholding a high standard of data protection by applying privacy principles such as notice, choice, access and accountability for onward transfer);

- Compliance with future **GDPR codes of conduct and certifications** (including when a non-EU entity voluntary decides to comply with such codes) or with **privacy codes of conduct and certifications** developed by other countries;

- **Publication of a transparency report** (for some organisations only) detailing numbers of accepted and rejected data government requests on a regular basis, as well as technical efforts to enhance security;

- Providing for **a backstop option to suspend** the transfer; and

- **Deciding to partially relocate some of the data in the EU** or deciding to move the data to alternative countries (adequate countries and/or countries with less risk of government surveillance) when technically possible, and when costs and risk assessments allow for it.

3. **Technical measures (except encryption)**

- **Comprehensive security infrastructure**, including: (i) state-of-the-art technical security measures to defend against third-party attacks and unauthorised access such as firewalls, antivirus, intrusion-prevention; (ii) regular auditing, testing and controls; (iii) access

[6] Organisations already apply this as a general rule across their processing operations as per Articles 5(c) and 25 of the GDPR.

controls and audit logging; (iv) physical security infrastructure; (v) application security and device management; and (vi) law enforcement ID verification;

- Policies requiring, on the basis of context and risk, enhanced security measures for **processing of sensitive data** (regardless of whether it is transferred outside of the EU); policies requiring enhanced security measures for transmission of information outside an organisation's internal organisation network (unless such measures are already part of the general security policies);

- **Anonymisation, pseudonymisation, tokenisation, data masking.** These techniques are used by some organisations to minimise the risk posed by the processing and could prove useful in some instances, but not all (especially where the techniques impact the effectiveness and usability of a data set, or when the service requires the use of non-anonymised data). In certain sectors, such as healthcare and pharma, anonymisation is applied by default as it is imposed by sectorial regulations;

- **Access restrictions** on the basis of data classification and/or on a case-by-case basis. These may have to be redefined on a long term basis to adapt information management systems;

- **EU Access Controls** where possible (e.g. access to data stored in the EU is limited to EU employees of EU entities; access from outside of the EU is reviewed, approved and supervised by an EU employee); and

- **Privacy-enhancing technologies and controls** (such as federated learning, or use of synthetic data, data sharding, computing encrypted data, etc.) may also reduce the risk of governmental access to data (although some of these are not yet fully available for commercial or wide-scale use).

4. Special considerations on relevance of encryption

- **Encryption is a privacy enhancing technique under the GDPR.** It is expressly recognised as an appropriate technical measure to ensure a level of security appropriate to the risk (Article 32; Recital 83). Encryption may be an appropriate safeguard that can render compatible any subsequent use of data for a new purpose (Article 6(4)(e)). Finally, encryption of data may be a technical protection measure relieving an organisation from an obligation to notify a data breach to a data subject (Article 34(3)(a));

- **Encryption is already widely used by organisations** in the context of their data processing activities to deliver appropriate data security and to mitigate risks of harms to individuals and the organisation, including in international transfer scenarios;

- **Encryption may be used to protect data at rest, data in transit, or both.** The details of the encryption method used may vary greatly depending upon its application, but the goal is to limit access to content to authorised parties;[7]

[7] There are circumstances in which regardless of encryption being used in transit and at rest, organisations can be compelled to assist with recovering of plaintext, no matter where in the world the data or the key might be stored (see EDPB opinion which effectively leaves organisations in conflict of laws situations https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en).

- **Encryption and decryption key management is important.** There are a variety of architectural and operational choices that organisations can make regarding how encryption keys are managed. Choosing the appropriate management approach requires an organisation to take into account potential security risks (as to whether the organisation is equipped to securely manage keys), operational risks (as to whether single points of failure are created for access to keys), unnecessary costs (from equipment required to manage keys) and functional limitations (as some services can have feature limitations with customer-controlled keys). Organisations need flexibility to implement the appropriate key management model for their particular scenarios, service functionalities and security risks involved;

- **Encryption is not a one-size-fits-all solution.** Organisations deploy encryption on a case-by-case basis based on the value, type and sensitivity of data; type of threats and risks to data, individuals and the organisations; likelihood and severity of harms; state of the art of technology; need of immediate availability of the data for the performance of the service; and the role of the organisation as a controller or a processor. The choice of encryption techniques and methodologies is always context-specific and may be different in the context of controller-processor or client and service provider relationship or commercial or corporate relationship;

- **Encryption cannot be used to protect against unauthorised access without functionality loss.** While encryption may work for data in transit and for data storage solutions and products, 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. While there is ongoing research on ways to process encrypted data (such as the ability to conduct AI modelling and algorithmic training on encrypted data), these techniques are not currently practical for most applications;

- **Encryption is only one tool in a larger toolbox of measures that organisations take** to reduce the instances and the risk of government access to data. Organisations use additional legal and organisational safeguards (as discussed above), as well as encryption, on a case-by-case basis. It is the totality of all of these measures that enables organisations to comply with the GDPR requirements on international data transfers;

- **Implementation of encryption across the corporate group may take a long time.** It may take several years for even a sophisticated global organisation to fully implement and reconfigure appropriate systems so that personal data that is subject to international data transfers is fully encrypted at rest and/or in transit; and

- **Some organisations face political pressure in the EU to not encrypt data.** Platform and communication organisations often face political and legal pressure from governments of the EU Member States to avoid encrypting data, or to provide “backdoors” to encrypted communications, so that data can be available to government security, intelligence and law enforcement agencies. This creates real tensions for the organisations if they are presented with conflicting messages and requirements from different regulators and different parts of governments in the EU.

5. **Measures specific to non-intra-group controller to processor relationships**

- **Publicly available transparency to business customers via "product transparency notices" or "privacy data sheets".** Depending on the product at stake and how it processes personal data, these are aimed to provide customers and clients with additional detailed information and reassurance about data privacy and security measures and compliance on a per-offer or per-product basis. These include information on where data is encrypted during transit and at rest;

- **Transparency** about third party hosting and processing locations;

- Depending on the service or product, service providers may allow clients to **choose where their data is hosted** and know where it is processed, including choosing to have data located and processed only in the EU; and

- **Cloud infrastructure providing customers the ability to define their own technical and operational measures** at the application layer, including access to servers and data (Private Cloud offers).

CIPL Recommendations:

- Provide a toolkit of outcome-based, illustrative, and possible supplementary measures for organisations to consider, choose and apply based on the context and risk;

- Rely on the GDPR risk-based approach for the choice and calibration of supplemental measures;

- Given the variety of data processing and transfers outside of the EU, do not provide for any hierarchy between the possible additional safeguards or supplemental measures organisations can implement;

- Do not impose a one-size-fits-all encryption requirement;

- Avoid prescriptive measures on the specifications or type of encryption technology required;

- Recognise the need for flexibility for organisations to deploy encryption based on context and on a case-by-case basis and acknowledge that the type, level and robustness of encryption should be appropriate to the type of threats, level of risk, type of data and processing and state of the art; and

- Acknowledge that encryption may not be a silver bullet solution and that it may not be relevant in all situations.

IV. ORGANISATIONAL ACCOUNTABILITY FRAMEWORKS AND PROCESSES FOR RESPONDING TO GOVERNMENT ACCESS TO DATA REQUESTS

Multinational organisations can be subject to many different local and foreign government requests for data for various purposes in the countries where they operate. These include requests for data in order to comply with applicable laws (such as HR, tax), personnel clearance to enter restricted areas, and also security intelligence requests and law enforcement requests (collectively "government access requests"). Some of these requests may carry potential criminal liability (personal and corporate) for non-compliance with legally binding orders served on organisations.

CIPL has found that a great majority of CIPL member organisations generally have global, comprehensive and accountable frameworks, policies and processes to respond to government access requests. These policies may be general and may not specifically address the situation where the requests occur in the context of a specific data transfer from the EU to a country outside of the EU. Other frameworks have specific provisions for responding to government access requests in the context of international transfer of data under the GDPR, in particular when such requests are frequent irrespective of whether they affect individuals in the EU or not. Some organisations even have pre-approved templates for release of information to law enforcement agencies with a subpoena or judicial request. These include policies that require the engagement of the privacy team if the request involves personal data. Some organisations also use online systems that allow verified government agencies to securely submit request for data access.

It is also interesting to note that some organisations do not currently have such frameworks in place because they are rarely or never subject to requests from government security and intelligence agencies. They are, however, ready to respond to these requests and would involve their legal teams (both local and global) and/or privacy team if personal data is involved, as well as additional functions depending on the request.

As an immediate consequence of the Judgment, organisations are reviewing their existing accountability frameworks for government access to data to ensure they meet the standards of the Judgment. These frameworks generally contain the following elements:

1. Organisational and governance measures

- Appointment of a **specific team and establishment of a governance and escalation structure** to handle government requests. These may involve different functions within legal, privacy, litigation, compliance, investigations, government relations and technology. It may also involve the Chief Information Security Officer and top senior corporate management if escalation is required;

- Setting up of **specific policies and procedures** and training of personnel to manage government requests governing: (i) the disclosure and provision of data pursuant to law enforcement/legal requests; (ii) the provision of metadata associated with communications; (iii) the notification and transparency to data subjects; (iv) the data retention and deletion protocols; (v) the legal challenge against data requests when deemed by the concerned entity to be unlawful or overbroad; (vi) emergency disclosure policies; and (vii) requiring processors to adopt a similar standard in responding to government access requests;

- Code of ethics requiring employees to **notify an** organisation **lawyer or other specialised and trained individuals** if they receive a government request for access to data; and

- Organisations generally make their approach to, and principles for, dealing with government data access requests **publicly available**[8] (unless prohibited to do so by applicable law).

2. **Review of government data access request**

- **Organisations conduct risk assessments** to consider the amount, type and sensitivity of the data, the nature of the request, the agency making the request, and the impact on the data subject (see section II);

- Some organisations **rely on international standards and frameworks** as the basis for assessing each request (such as the UN Human Right Council's "protect, respect and remedy" framework and guiding principles, the Telecommunications Industry Dialogue guiding principles or the Global Network Initiative principles and commitments[9]); and

- Organisations conduct **legal analysis** to verify that any request received from a competent authority complies with the judicial/legal processes that correspond to the country in question (i.e. are based on a valid statutory basis, have a valid court order, warrant, subpoena, request in writing on official letterhead and signed by a law enforcement authority). Organisations often reject or require greater specificity on requests that appear overly broad or vague. Some requests may also be challenged in court.

3. **Responding to government data access request**

- **Use of appropriate security measures** to securely transmit information; and

- Inclusion of a cover letter to remind the recipient of the data minimisation principle and setting out the **expectations for use limitations** and protection of the data by the recipient.

4. **Actions taken after addressing the government data access request**

- **Documentation and recording** of the request received and response provided;

- **Reliance on experts such as third-party consultancies and NGOs** to help organisations monitor and report government access to data (such as Business for Social Responsibility; Business & Human Rights).

---

[8] https://www.telefonica.com/documents/1258915/1261648/summary-global-rule-requests-competent-authorities-19.pdf/a12df9c2-75d2-70b3-37dc-df920002f5bd
https://www.telefonica.com/documents/153952/183394/Report-Transparency-Communications-2020.pdf/826611a3-7204-6ec9-e3d2-f4be7d4f87a5
https://www.ibm.com/blogs/think/2014/03/open-letter-data/
https://www.ibm.com/blogs/policy/trust-principles/
https://transparency.facebook.com/government-data-requests
https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report
https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report
https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF

[9] https://globalnetworkinitiative.org/gni-principles/

- **Publication of regular transparency reports**. A few organisations publish regular transparency reports that summarise information regarding government access requests they receive around the world with the granularity required under applicable law (including requests received regarding legal interception, access to metadata, blocking and filtering of contents and suspension of the service). Such transparency reports generally cover all the countries in which the organisation operates. These reports can differentiate between responses to national security intelligence and surveillance requests on the one hand and law enforcement requests on the other hand.[10]

5. **Specific actions of processors to respond to government access requests on client data**

Processors handle data on behalf of, and on the instructions of, their clients. These clients can be private organisations as well as public entities. Processors are generally bound by contractual provisions or terms of service that may be breached if they have to respond directly to government requests. Consequently, processors generally expect that government requests to access client data (regarding for instance their employees, users or customers) would go directly to their clients (who are generally the controllers of such data).

In case they receive a direct government access request, they could for example commit to the following steps to protect their customer's interests in case this does not lead to a conflict with the laws of the third country:

- **Transparency** of organisations acting as processors towards their clients concerning their commitments to respond to government data access on client data;

- **Public commitment** that the organisation: (i) has not provided client data to any government agency under any surveillance program involving the bulk collection of content or metadata; (ii) does not put "backdoors" in its products for any government agency, nor does it provide software source code or encryption keys to any government agency for the purpose of accessing client data, (iii) does not provide unlimited and unfettered government access to its data; (iv) does not provide any government with encryption keys or the ability to break the organisation's encryption;

- **Notification of the client** upon receipt of a legally binding request for disclosure of data (so that the client may attempt to limit or prevent disclosure), unless applicable law prohibits notification;

- **Challenge of requests** that prohibit notification to the client through appropriate legal process or other means;

- Only provide such data if the **government agency has appropriate statutory authority** under applicable law to require the processor to provide such data (such as a valid warrant or court order);

[10] For government access in the US specifically, organisations report the number and nature of U.S. national security data requests, including breakdowns of Foreign Intelligence Surveillance Act ("FISA") orders that seek the content of accounts or non-content information (such as subscriber name) and the number of National Security Letters received. Pursuant to US Department of Justice requirements, these numbers are reported within ranges of 500 and FISA requests are subject to a six-month reporting delay.

- **Seek to narrow any government access request** on client data to only the specific information required to respond (including by using judicial means);

- **To the extent permitted by applicable law, notify the competent DPA** as part of approved BCR (if the request is likely to have a substantial adverse effect on the guarantees provided to the data subject under EU law);

- **Challenge government requests** and ask the public entity to invoke the **mutual legal assistance treaties** where compliance with a valid government request for client data would put such organisation in potential breach of applicable data protection law in another country that has jurisdiction or authority over the client data; and

- Provide for **narrow exceptions in emergency cases** (e.g. criminal activity) where disclosing client data would prevent imminent death or serious physical harm to an individual. In this case, the processor notifies the client promptly and includes that disclosure in its transparency report. The processor only provides the data believed to be strictly necessary to enable the government authority to address the emergency.

CIPL Recommendations:

- Recognise that organisations may be exposed to criminal liability for non-compliance with government access requests;

- Acknowledge that accountable organisations typically will have built and implemented robust frameworks to satisfactorily mitigate the risk of government access to data and further encourage organisations to do so;

- Recognise that accountability frameworks for government access to data requests can be a supplementary measure in addition to legal, organisational and technical safeguards; and

- Recognise that some organisations never or rarely receive government requests for access to data.

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