Centre for Information Policy Leadership
Hunton & Williams LLP

13 October 2017

CENTRE FOR INFORMATION POLICY LEADERSHIP RESPONSE

CONSULTATION BY THE IRISH DATA PROTECTION COMMISSIONER ON THE TOPICS OF TRANSPARENCY AND INTERNATIONAL DATA TRANSFERS UNDER THE GDPR

The Centre for Information Policy Leadership at Hunton & Williams LLP (CIPL)[1] welcomes this opportunity to respond to the Irish Data Protection Commissioner (DPC) on its consultation on transparency and international data transfers under the GDPR.

This response addresses a selection of questions on which the DPC is seeking input. The selection is based on the applicability of a question to CIPL's perspective as a privacy and data protection think tank and also on CIPL's specific expertise in relation to transparency and international data transfers.

CIPL attaches as an annex to this submission:

- The transparency section from CIPL's white paper on Recommendations for Implementing Transparency, Consent and Legitimate Interest[2];
- CIPL's white paper on Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms[3]; and
- CIPL's recently revised and updated paper on Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy.[4]

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton & Williams LLP and is financially supported by the law firm and 56 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 at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton & Williams.

[2] http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf.

[3] http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf.

[4] https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper__final_-_essential_legislative_approaches_for_enabling_cross-border_data_transfers.pdf.

Transparency

Question 1: There is no definition of transparency under the GDPR, although Recitals 39 and 58, amongst others, are informative as interpretative guides. How should transparency be defined/interpreted?

Answer:

Deciphering how transparency should be defined or interpreted under the GDPR starts with understanding the goals of transparency. CIPL takes the view that there are three core aims of implementing transparency.

1. Transparency seeks to provide appropriate information to individuals to ensure processing is fair and to enable their informed engagement, exercise of rights under the GDPR and, where relevant, valid consent.

2. Transparency seeks to create an awareness of an organisation's information practices in a way that promotes individual trust, deepens the customer relationship, alleviates any concerns about the use of personal data and ensures proper understanding of and potential "buy-in" to the value propositions of data use by the organisation.

3. Transparency also has a role to play vis-à-vis the general public, policymakers, legislators and data privacy regulators. As such, it is an important element of organisational accountability.

In CIPL's view, the transparency requirement in the GDPR is broader than privacy notice requirements under Articles 13 and 14 of the GDPR. Transparency in the GDPR has to be addressed by organisations in respect of the following:

a) Transparency is now an explicit requirement and part of the first data protection principle — personal data must be processed fairly, lawfully and in a transparent manner (Article 5(1)(a); Recital 39). Transparency is linked to and an integral part of the fairness principle. In order to ensure processing is fair to individuals, organisations must comply with the transparency requirement and especially privacy notice requirements under Articles 13 and 14.

b) Transparency also means that a controller must provide information and all communications to individuals in a concise, transparent, intelligible and easily accessible form, using clear and plain language (Article 12(1)). This is required especially in respect of the following instances of communication with individuals:

    – Providing privacy notices to individuals when data are collected from individuals (Article 13) or from third parties (Article 14);

- Responding to individuals exercising their individual rights under GDPR: right of access (Article 15); right of rectification (Article 16); right to erasure (Article 17); right to restriction (Article 18); notification regarding rectification, erasure or restriction (Article 19); right to data portability (Article 20); right to object (Article 21); and rights in respect of automated decision-making (Article 22);

- Notifications to individuals of and regarding personal data breach when it is likely to result in a high risk to the rights and freedoms of that individual (Article 34).

c) The guidance in Recitals 39, 58 and 60-63 provides the "spirit" of the GDPR transparency requirements and also illustrates that transparency is contextual. In general, individuals must be made aware of processing, purposes of processing, risks, rules, safeguards and rights in a way that enables them to take part in digital life with confidence. This does not mean that this information is always necessary or required. Rather, it depends on context what precise information and how much of it is to be provided to the individual. In some instances it may be appropriate to mention the risks of processing (e.g. the fact that data will be shared with others, or posted publicly). Equally, in some instances it may be appropriate to provide more information about the safeguards the organisation implements to mitigate specific risks, or to clarify how the organisation's reliance on the legitimate interest ground does not prejudice individuals' rights.

d) Transparency is also linked to and an integral part of GDPR requirements for: i) consent (consent must be informed in order to be valid); ii) legitimate interest processing (individuals must be informed about the legitimate interest of the controller or third party); and iii) publicising of DPO contacts (to the DPA and wider public).

CIPL has been active in advocating for a new approach to transparency, one that is user-centric and promotes effective engagement and trusted relations with individuals, rather than solely focusing on legal compliance with the strict requirements of Articles 13 and 14, for example. Providing detailed terms and conditions and privacy notices is necessary for compliance with legal transparency, but user-centric transparency is essential to ensure the goals of transparency are met through effectively promoting understanding to individuals. Organisations need to step up and create effective and innovative ways of interacting with individuals and providing necessary information, with the help of multidisciplinary teams of technologists, user design specialists, behavioural economists, marketers and lawyers. CIPL recognises that this may be difficult for SMEs, startups and many other organisations that don't have the resources to access such multidisciplinary teams. As a result, guidance showcasing best practices and available tools to deliver user-centric transparency must be made available by DPAs so that such organisations can also step up and provide effective transparency.

Question 2: Article 12(1) of the GDPR requires a data controller to take "appropriate measures" to provide the information required under Articles 13 and 14 and any communications under Articles 15–22 and 34 relating to processing, in accordance with the transparency requirements set out in that Article. In other words, the information / communication in question should be concise, transparent, intelligible, easily accessible and use clear and plain language.

What factors should be taken into consideration when determining what may be "appropriate measures" for these purposes? What sorts of transparency tools/techniques/ mechanisms/approaches might constitute "appropriate measures" for these purposes?

Answer:

When considering what may be appropriate measures to deliver transparency under the GDPR, CIPL believes that organisations and DPAs should take into account the following:

a) How to stay true to the spirit of the law and the objectives of transparency. Long legalistic privacy notices may comply with the strict letter of GDPR, but may not deliver real transparency to individuals and achieve the core goals we mention above.

b) Prevalence and prominence should be given to information that is actionable, or otherwise really useful for individuals (to reassure them about data use or enable them to make choices). Also, information about what an organisation will not do with data may be more powerful and important in some circumstances than trivial or obvious information about what organisations do as a matter of course.

c) Information should be provided in a timely manner when and where it is most meaningful to individuals. This can be done through a "push" model where organisations proactively provide information to individuals as they interact with different services on a "just-in-time" model, or through a "pull" model where organisations make information available to individuals at their convenience.

d) Information can be provided in a layered format[5] and in multiple locations and places, including just-in-time notices, pop-up boxes and broader privacy policies.

e) Communications to individuals should be innovative, using multiple platforms and means, embedded in the products and services, including in one-stop dashboards and privacy management apps or sites, in line with the services being provided and the expectations of the individual.

[5] See Section 5 of the Spanish DPA guidelines on the GDPR's duty to inform, published February 2017. https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/modeloclausulainformativa.pdf.

f) Organisations should deploy multidisciplinary teams to work on information provision and communications with individuals, especially user design experts, marketers, economists and technologists to determine the best way to deliver user-centric transparency. SMEs and startups should refer to best practices to make such determinations where they do not have the required resources to engage such multidisciplinary teams. Cost should not be a barrier to delivering effective transparency.

g) However, it is also important that data privacy supervisory authorities incentivise and allow more flexibility and innovation in the way organisations comply and deliver transparency under the GDPR, taking into account that there are vastly different types of organisations from startups to multinationals.

h) Finally, the actual costs to the controller of delivering transparency through available mechanisms should be taken into account. Controllers, especially SMEs and startups, cannot be expected to incur disproportionate costs in delivering transparency in certain situations, especially where information is obvious to individuals. For example, a company that merges with another and acquires a large database of customer data might incur disproportionate costs if it must individually notify every customer of the acquisition. In such a situation, a general announcement on the company website still ensures delivery of transparency but in a more cost-effective manner. Similarly, a customer call centre taking calls from customers wishing to purchase a product may find it disproportionate and lead to customer annoyance and loss of business to provide a full privacy notice at the time of first contact and data collection, especially where research shows that calling customers do not want to spend any time or cost listening to upfront long privacy notices. There should be flexibility in how the transparency requirement is interpreted, including in terms of modalities and timing of communications with individuals.

Question 5: Article 12(7) provides that the information which is to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons. Article 12(8) provides that the European Commission is empowered to adopt delegated acts under Article 92 for the purposes of standardising the use of icons. What categories of information, to be presented by the use of icons, should be prioritised for the standardisation of icons?

Answer:

CIPL believes that icons might be able to provide useful information and create market value in some cases, for instance, among generations that have grown up with apps and digital symbols and for educators who could use icons to promote digital safety to children. However, CIPL also notes that there is significant scepticism in the marketplace (among NGOs, consumer associations and consumer-facing businesses) as to the viability of this concept as a transparency tool. Icons tend to be static, describing a fixed practice, and therefore not suitable

for modern data processing that tends to be dynamic and constantly evolving with innovation. Such changes cannot be captured in real time by simplistic and fixed icons. Additionally, if there are too many icons, they will not simplify or promote user-centric transparency for individuals and may in fact be perceived as burdensome and confusing if individuals have to learn the meaning of many different icons.

CIPL believes that, should icons be employed as a transparency mechanism, they should not be created and imposed "top down". Where possible, icons should be initially developed by industry, based on market and consumer research, and then vetted, refined and potentially harmonised in collaborative stakeholder processes. However, organisations should also have the flexibility to create and deploy their own icons to suit their brands' products and services. The use of icons should be limited to where it makes sense, where processing is fixed and consistent across sectors for some basic practices.

Finally, it is difficult to see how icons can realistically be standardised across different subject matters and applications, suiting all categories of individuals (customers, employees and citizens) and all different data uses and alternative platforms. However, harmonisation should be encouraged where possible so as to avoid confusion of individuals having to learn the differences between different icon systems.

Question 6: Article 13 sets out the information which must be provided to a data subject where personal data "are collected from the data subject" while Article 14 sets out the information which must be provided to a data subject "where personal data have not been obtained from the data subject". Which of Articles 13 or 14 should apply (and why) where:

a. Personal data is collected remotely/passively from a data subject i.e. it is collected from, or on, the data subject but without the data subject actively providing it to the data controller e.g. it has been collected by way of observation, CCTV recording, Bluetooth "beacons" or Wi-Fi tracking of the data subject?

b. Further personal data is inferred, derived or generated by a data controller from a set of personal data which was originally provided directly by a data subject to a data controller?

Answer:

Consistent with the fairness principle of the GDPR, CIPL believes that the notice requirement should cover and applies to passively collected and observed data. In addition, it should cover data that was inferred or derived under Article 14 of the GDPR, subject to applicable exceptions and appropriate to timing. Normally organisations should provide the relevant information at the time of first contact with the individual, in as much as it is possible to anticipate the future processing of data at that point. This can be done in a specific privacy notice at the time of first contact, or in a more general privacy policy on a website referred to at the point of contact. In other words, relevant information about processing of passively collected and observed personal data can be combined with the information given at the time of collection of data.

However, this does not preclude the organisation from providing subsequent notices at a later time, if it is appropriate to inform the individuals about a specific processing of passively collected and observed or derived and inferred data which has not been anticipated at the time of first contact and data collection. In other words, there must be flexibility in interpreting the transparency requirements in this context to allow organisations to provide the necessary information as and when it is most appropriate and useful for the individual. This is consistent with our view that transparency is a matter of digital and individual trust and deepens the customer relationship. As such, it has to be dynamic and not static, as this could create risks to processing for certain purposes such as data analytics which can benefit individuals.

Question 8: Recital 39 refers to the provision of certain information which is not explicitly covered by Articles 13 and 14 of the GDPR and specifically that "natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data." What information (other than that set out in Articles 13 and 14) should be provided by data controllers to data subjects in connection with the "risks, rules, safeguards and rights"?

Answer:

CIPL is of the view that compliance with Articles 13 and 14 of the GDPR already fully meets the obligations of disclosing risks, rules, safeguards and rights in relation to the processing of personal data. As we mention above under our answer to Question 1, some processing operations may require further specific disclosures of information to individuals. In these cases, the provision of such information should be left to the judgement and discretion of the organisation concerned. Organisations should add to the information requirements of the GDPR only where necessary and where this is reasonable in light of the fair processing requirement. The point of the interpretative guidance in Recital 39 is to capture the spirit of transparency, rather than rigidly add further and more specific privacy notice elements.

Question 9: The exceptions to the information requirements under Article 14(1), 14(2) and 14(4) are set out in Article 14(5). These include: where "the provision of such information proves impossible or would involve a disproportionate effort..." (Article 14(5)(b)); and where obtaining or disclosure of the personal data is expressly laid down by EU or national law to which the data controller is subject and which provides appropriate measures to protect the data subject's legitimate interests (Article 14(5)(c)).

a. How should the concept of "impossibility" be interpreted in accordance with Article 14(5)(b)?

b. What should constitute a "disproportionate effort" in accordance with Article 14(5)(b)?

c. Should the reference to the EU or national law referred to in Article 14(5)(c) be interpreted as meaning that (i) the law requires the data controller to obtain or disclose the personal data on a mandatory basis or (ii) the law allows for - but does not make obligatory - the obtaining or disclosure of personal data?

d. What should constitute "appropriate measures to protect the data subject's legitimate interests" in the EU or national law referred to in Article 14(5)(c)?

Answer:

There will be situations where a provision of privacy notice and information under Article 14 is not appropriate and should be covered by the exemption in Article 14(5). For example:

a) It may be impossible to provide a notice to individuals with whom a controller does not have a relationship (e.g. coded data for the sponsor of a clinical trial, or IP addresses or location data for providers of mobile phone hardware/chips), nor a means of contacting them, without acquiring more personal data or breaching the law. These situations are becoming more numerous in the modern digital economy. If all companies that collected data from third-party controllers had to contact consumers directly there would be an explosion of communications received by the individuals who would likely find them confusing or frustrating. This would serve no public interest purpose if the use of their data carried no risks or any risks had been mitigated.

b) It may defeat the purpose of processing to provide a notice about processing of personal data to a potential or actual fraudster, or hacker, or an employee who is leaking company intellectual property. This would prejudice the actual processing objectives. These situations should be covered under the "impossibility"/ "disproportionate effort" exemption.

c) There will be circumstances where a provision of detailed information under Article 14 is disproportionate because of the trivial, common or reasonably foreseeable use of data. Also, the risk-based approach in the GDPR should allow for organisations to tailor their privacy notices based on the level and likelihood of risks to individuals. This also means that where data processing is common and does not create any risks (or any risks have been mitigated) to individuals, the provision of the notice may be disproportionate, or such notice can be shorter, or provided on a pull model, as opposed to a proactive push. Examples of these cases would include when an employee provides next-of-kin information to HR for emergencies or beneficiary information for pension or disability purposes. It would be disproportionate for an employer to inform the employee's spouse that he or she provided the information. Another example would be where one organisation partners with another to invite their business customers to an event or conference and obtains the customers' email addresses from the partner organisation to send out invitations. It would be disproportionate for the organisation to provide a notice to individuals in this scenario.

d) Finally, the number of individuals and how easy it is to reach out to them (in terms of time, technology and costs) and provide the required information is relevant in determining whether the effort of providing the notice is disproportionate, especially

where the processing carries no risks or any risks have been mitigated. In situations involving large numbers of individuals, alternative notice such as publication through national media may be useful and reasonable. Furthermore, guidance from DPAs regarding the disproportionate effort principle based on scenarios they see could provide insights for companies on when and where its use is most appropriate. Organisations, along with considering the DPA guidance, will also have to demonstrate accountable use of the disproportionate effort exception, including being able to demonstrate to a DPA in the case of an investigation the thought processes behind using it.

With regard to Article 14(5)(c), the reference to EU or national law should be interpreted as meaning both that (i) the law requires the data controller to obtain or disclose the personal data on a mandatory basis and (ii) the law allows for — but does not make obligatory — the obtaining or disclosure of personal data.

- Article 14(5)(c) always applies if the law imposes such disclosure. For example, when a court order or police, antitrust or tax authorities require the data controller to provide the personal data according to the competences granted to such authorities by applicable law or when a competent authority is imposing a change of controllership (e.g. a divestment imposed by an antitrust authority in a concentration proceeding). Another instance where Article 14(5)(c) applies is where the law imposes transparency duties, such as where payments are made to healthcare professionals by the pharmaceutical industry or in the need to gather information from reliable third-party sources for anti-money laundering purposes and its disclosure to antitrust or financial authorities.

- However, there could be situations in which criteria under scenario (ii) above apply. For example, the change of controllership arising from a transaction regulated by a law that does not impose informing data subjects individually of the change of entity provided the data processing carried out by the new controller is limited to the same or compatible processing purposes. This would likely occur in cases of merger, spin-offs, a securitisation or transfer of credit rights. Another example could be the obtaining or disclosure of information that is appropriate for the establishment, exercise or defence of a legal claim (before an administrative, judicial or arbitration body), such as the obtaining and disclosure of a medical report by an individual and his/her lawyers to submit a valid incapacity claim regarding a relative.

Question 10: How can information "fatigue" (which would undermine the positive benefits of transparency for the data subject) be avoided by data controllers while still ensuring compliance with all of the transparency requirements in the GDPR?

Answer:

Information fatigue can be avoided while still ensuring compliance with all transparency requirements by:

a) Embedding transparency mechanisms as much as possible within the relevant product, service, process or technology. By integrating transparency into products and services, individuals will receive information in a more seamless and less interrupting fashion as they use and interact with different technologies.

b) Providing the right amount and critical information upfront, with an option to view further information should the individual so desire. There is a tension between the legal requirement to provide detailed notices to individuals for each data processing with a long list of prescribed content (as required under Articles 13 and 14) and the requirement that the notices be clear, concise and user friendly. Providing long and complicated notices defeats the purpose of transparency (which is to provide understandable and actionable information to individuals) and can cause fatigue through information overload. Providing actionable and targeted user-facing information focused on individuals and their needs, based on a "push" model, and more detailed legal disclosures upon request or on a different section of a website, based on a "pull" model, is one way of ensuring that individuals receive the critical information upfront without being overburdened with the technical and legal language of more traditional notices.

c) Delivering transparency by different methods and at different times, appropriate to context. For example, when an individual is signing up to use an online service to file their taxes, it is appropriate to display in clear and concise terminology, at the time of sign-up, that the information they enter on and collected by the site may be processed and used to produce an automated decision which could have a legal effect on that individual. In contrast, notifying a user every time they are shown an online ad that their data is being processed to display the ad would be inappropriate and may lead to the individual abandoning the service out of frustration from constant interruption. In this case, it would be more appropriate to allow the user to find all the relevant information about online ads in the ad settings service of the site they are using. This ensures transparency is delivered by an appropriate method (in the ad settings) and at the appropriate time (on demand).

d) Ensuring flexibility in how organisations provide information to individuals. It would be helpful for any guidance to clearly specify and allow the use of layered notices, splitting information between specific notice/just-in-time notice and a more general privacy

policy available on demand. Also, there must be flexibility on how the elements of notice in Articles 13 and 14 are interpreted. It is unrealistic and will lead to notice fatigue if a notice has to specify different retention periods for every single data point, or if a privacy policy has to explain every single use of the legitimate interest processing ground for different data and purposes. This will make notices and policies even more unwieldy.

e) Finally, making full use of exemptions to the notice requirements in the GDPR (under Article 14) and any further exemptions at member state level (based on Article 23) — as we discussed under Question 9. The raison d'être of these exemptions is also to avoid user fatigue and excessive provision of privacy notices.

International Data Transfers

Question 1: Which legal bases/mechanisms for conducting personal data transfers to third countries or international organisations under the GDPR are likely to be most commonly relied on by your organisation?

Answer:

In October 2016 CIPL published a report from the first GDPR benchmarking survey that CIPL conducted together with AvePoint. With over 220 organisations responding, we asked participants to specify their grounds for data transfers today and after GDPR comes into force (for transfers of HR and customer data and transfers of data to vendors). In summary, the results show that:

- At present, the most popular tools for legitimising international data transfers are model clauses (used by two-thirds of organisations), followed by consent, necessity of contract and the Privacy Shield.

- Post-GDPR, organisations will rely less on consent for transfers of HR and customer data. In addition to model clauses, which remain popular, the results indicate that there will be a swing towards increased use of BCR (21-28% of organisations), controllers' legitimate interests (a quarter of organisations) and the Privacy Shield (21-27% of organisations).

CIPL is currently conducting the same survey and we expect to have the full report by the end of 2017. We will share the results of the survey, including in respect of this particular question, with the Irish Data Protection Commissioner.

CIPL also believes that some of the derogations under the current Directive are commonly used by organisations today, and that will continue under the GDPR. One such example is the establishment, exercise or defence of legal rights and claims. Article 48 of the GDPR states that

any judgment of a court/tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty (MLAT), in force between the requesting third country and the Union or a member state, without prejudice to other grounds for transfer. Indeed, in practice, the public interest, as well as the establishment, exercise or defence of legal claims are the grounds that are mainly applied for such situations under Article 48 (discovery, antitrust audits, etc.). MLATs are uncommon and unrealistic for transfers connected to administrative or judicial claims on non-criminal matters.

Finally, as discussed, below, we expect that certifications and codes of conduct would also be a route explored by industry and specific sectors to legitimise international transfers, based on specific safeguards of the relevant sector imposed by sectoral regulations or voluntary commitments of its members.

Question 2: What are the challenges to conducting personal data transfers to third countries or international organisations under each of the available legal bases/mechanisms set out in the GDPR?

Answer:

There are a number of challenges associated with the various mechanisms for international data transfers:

1. **Standard Contractual Clauses (SCC)**: SCC are widely used by many organisations, especially for data transfers between EU controllers and non-EU processors and for intragroup transfers, despite some practical challenges. The practices and challenges will continue under the GDPR, although the GDPR has streamlined the use of SCC and gotten rid of national authorisations and submission of SCC to DPAs.

    a. SCC are not flexible enough for multinational companies (with multiple controller and processor affiliates and third parties) or for modern global business processes (outsourcing, cloud and IT services) with multiple and changeable transfers and numerous controllers, processors and sub-processors.

    b. Organisations feel they are spending too much time on the bureaucracy of setting up the network of SCC for each processing and transfer operation and executing the SCC, rather than on putting resources towards actual data privacy compliance underpinning each contract.

    c. With forthcoming legal challenges to SCC in the Court of Justice of the European Union (CJEU), organisations have serious concerns about their ability to continue to use this mechanism going forward and the impact the challenges may have on their business processes, business partner relationships and digital and data

strategy. This legal uncertainty is even more exasperated, given the geographical limitations of Privacy Shield (covering only transfers to the United States) and the administrative burdens of the BCR approval process.

d. Despite the current legal uncertainty, should SCC remain a valid data transfer mechanism they will have to be brought in line with the GDPR. There will be substantial amounts of administrative work involved for many companies as they seek to update their existing contracts based on SCC (for large organisations, this potentially means hundreds and thousands of contracts). The practical difficulties, if not impossibility, of having all of these contracts up to date in a quick timeframe should be acknowledged by DPAs. Companies should be able to rely on their existing SCC with a reasonable time frame for updating them to the new SCC once they are available.

e. Another challenge associated with data transfers under SCC is that there are currently no processor-to-processor SCC which would allow European processors to transfer data lawfully to non-European processors and sub-processors. At present, organisations deal with this either by ensuring that the controller enters into stand-alone SCC with non-EU processors/sub-processors or by giving an EU-based processor a power of attorney towards non-EU processors and sub-processors. This creates a great deal of administrative work for all parties. The situation will be even more complex under the GDPR, with processors having a new obligation to comply directly with GDPR international data transfer requirements. It is imperative that workable and commercially viable solutions are created to enable lawful transfers between EU-processors and non-EU processors/sub-processors, given the use of multiple processors and sub-processors in many modern-day processing operations. CIPL believes that this should not necessarily be created by the Commission and/or WP29/EDPB, but instead that the relevant industry should lead the creation of model terms and clauses to cover processor-to-processor data transfers. Alternatively, the accountability principle may be used to enable such transfers where each processor remains accountable and responsible to ensure compliance and the protection of personal data by any other non-EU processors and sub-processors.

2. **Binding Corporate Rules** (BCR): While this mechanism seems to be gaining popularity, it is still perceived as a gold-plate approach, suitable for large organisations with large resources, a dedicated DPO and large teams. We believe that BCR need to be made scalable, to facilitate wider use that is not limited to only the largest organisations.

   The key challenge is rooted in the need for approval of BCR by a DPA and a slow review and approval process, that also varies by DPAs, depending on their experience and workload (although some real progress and improvement have been made in the past couple of years). If BCR are to be used by many more organisations, then the review and approval process needs to be streamlined further and perhaps changed substantially.

CIPL believes that ideally and in the long run, BCR should not require prior approval by DPAs. Rather, BCR should be based on a self-certification system, or on a review by a third party (an accredited certification body under the GDPR, or an "Accountability Agent" as in the APEC CBPR system), with companies ready to demonstrate their BCR and compliance to DPAs on request.

However, Article 47(1) of the GDPR still requires that BCR be approved by a competent supervisory authority. Given this requirement, CIPL recommends:

i. The BCR approval process be further streamlined and improved to facilitate faster processing times. This means that DPAs will have to dedicate more resources to BCR review and approvals. They will also have to ensure better sharing of information and expertise between different DPAs on this topic.

ii. BCR should not be viewed exclusively as a transfer mechanism, but as a demonstration of accountability under the GDPR. For a great majority of BCR-approved companies, this is already the case, as BCR represent the actual privacy compliance program that they deploy across their group of companies.

iii. BCR should be leveraged and "upgraded" to GDPR certification under Articles 42 and 43 of the GDPR. De facto, BCR are already a form of certification for a company's privacy compliance program and act as a "badge of recognition" by DPAs. This is how most BCR companies view their BCR, both internally and externally, and how their business partners view the BCR, too.

iv. Companies that update their BCR to be in compliance with the GDPR should not be required to go through another comprehensive review and re-approval process, but should have a special "fast track" process of updating their BCR in line with the GDPR and future GDPR certifications.

v. CIPL believes that there is scope to develop and evolve the BCR mechanism further under the GDPR to align it with the latest developments on international data transfers. As discussed, most organisations (both controllers and processors) view BCR not only as a transfer mechanism, but also as a privacy compliance program that includes all the necessary elements of accountability under GDPR. The organisations apply BCR rules across their group of companies to ensure a uniform and high level of privacy protection. DPA approval of the BCR is equally viewed as a "seal of approval" and recognition of the commitment of the organisation to data privacy compliance. As such, there is potential for BCR to evolve into GDPR certification, as discussed in this document. Equally, if BCR are viewed as a "badge of recognition" for a company's privacy compliance program and receive approval by DPAs, then any data transfers to a BCR approved company and also between BCR approved companies should be

allowed based on BCR compliance by the company or companies and without any additional transfer mechanism (model clauses or derogations, for example). If transfers from Europe to a US based Privacy Shield certified company can take place based on self-certification with Privacy Shield, then transfers from the EU to a BCR approved company should also be allowed. Therefore, CIPL believes that the next logical step in the evolution of BCR would be as follows:

a. International data transfers should be permitted to take place (without additional transfer mechanisms in place such as model clauses or derogations) between two BCR approved companies (either controllers or processors), as both companies will have high levels of privacy protection within their groups in respect of all the data they receive and share. This would mean that specifically controller to controller and processor to sub-processor transfers should be permitted.

b. International transfers from any controller (not BCR-approved) to a BCR-approved controller should also be permitted, without a need for model clauses or derogations.

CIPL will continue to work with interested and accountable organisations and DPAs and the Commission in exploring these options and how they may work in practice with the changes brought by the GDPR.

vi. The GDPR expands the application of BCR from use within a corporate group to a group of enterprises "engaged in a joint economic activity". The GDPR does not define the meaning of "engaged in a joint economic activity". We believe that this term could be interpreted broadly to cover various scenarios discussed above where two groups of companies engage in a formal or commercial and contractual relationship, in respect of a provision of service, development of a product or a joined collaboration or activity which involves some data sharing between two organisations.

vii. Finally, in light of Brexit, it is important to ensure that there is continuity in the way BCR work in the UK and the rest of the EU, both from procedural/approval aspects and substantively.

3. **Certifications and Codes of Conduct**: The GDPR specifically encourages the development of certifications and seals, as well as, codes of conduct and their use as mechanisms for managing and legitimising cross-border data flows. These mechanisms appear promising and, if implemented properly, will address the efficiency and flexibility challenges associated with SCC and BCR.

a) It is imperative that there are sufficient incentives and benefits for organisations to consider GDPR certifications and codes of conduct, in addition to the many certifications that they already pursue (e.g. ISO, or CBPR, or other national privacy

seals/marks). If these benefits are not clear, organisations will approach certifications and codes of conduct as yet another administrative cost and not make the most of them.

b) The certification process must be scalable and affordable, for all sizes and types of organisations.

c) There should be a reasonable expectation to have a code of conduct approved in a short and predetermined period of time.

d) Certifications and codes of conduct for data transfers must be developed at EU level and must work in all EU member states.

e) Regarding certifications only, the ultimate goal should be to facilitate the interoperability of GDPR certifications with other transfer mechanisms such as the APEC CBPR and other relevant certifications (ISO standards, Japan Privacy Mark, etc.). New transfer-related certifications should, where possible, avoid creating conflicting substantive and procedural requirements with other systems. Many global companies have a single privacy management program and must leverage this program to obtain Privacy Shield certification in the US, CBPR certification in APEC and BCR in Europe.

Question 3: **What specific actions might the Article 29 Working Party and/or national data protection authorities take to help organisations address or alleviate such challenges?**

Answer:

We include the answers to this question in our answers to question 2 above. In addition to those comments, the WP29 and DPAs can:

a) Ensure a common interpretation of the derogations. This is particularly important where large organisations have "multinational" IT systems that deal with personal data from multiple countries as differing interpretations will lead to the derogations becoming unworkable in practice;

b) Acknowledge the need for a flexible interpretation of the derogations (e.g. the establishment, exercise or defence of legal claims); and

c) Work with industry to find solutions to some common key issues on data transfers that are not addressed by any of the derogations.

Question 4: What aspects of international personal data transfers under the GDPR should be prioritised for the purposes of guidelines which may be produced by the Article 29 Working Party and/or national data protection authorities?

Answer:

CIPL believes that the most immediate actions and tactical priorities in respect of international data transfers are as follows:

a) WP29 and the Commission should work on updating the existing SCC in light of the GDPR and bearing in mind the current legal challenges to SCC in CJEU. WP29 should provide interim guidance to organisations to address their fear of lack of legal certainty and reassure the market (including foreign controllers and processors) about the validity of SCC in the interim and how to smoothly transition from current SCC to updated SCC.

b) Upgrade BCR to reflect new GDPR requirements and transform BCR to GDPR certifications, certifiable by accredited third parties. Ensure existing BCR-approved companies do not have to go through the full-blown approval/certification process again.

c) Ensure that BCR can be used to legitimise data transfers in the scenarios described under the answer to question 2, point 2, sub-point (v) of this response (See pages 14 and 15).

d) Working with relevant industries, address EU processor to non-EU processor/sub-processor transfers (taking into account the criticism of the P2P model clauses drafted by the Spanish DPA[6] and the Working Document 01/2014 on Draft Ad Hoc Contractual Clauses "EU data processor to non-EU sub-processor"[7]).

e) Together with the Commission, continue to work with APEC on exploring and building interoperability between transfer mechanisms such as CBPR, BCR and GDPR certifications. To the extent possible at this early stage, any guidelines that are going to be produced now should anticipate potential future interoperability solutions.

f) Together with industry and relevant think tanks, work on best practices and tools to address the personal data transfers under Article 48 of the GDPR that fall under the public interest and legal claims derogations (e.g. discovery procedures, antitrust proceedings, etc.).

Question 5: If there are other aspects of international personal data transfers under the GDPR on which you have specific comments, proposals or questions (whether legal, practical, interpretative or otherwise), please provide us with this feedback.

Answer:

[6] https://www.agpd.es/portalwebAGPD/resoluciones/autorizacion_transf/common/pdfs/MODELO-DEFINITIVO-AEPD_Contrato-encargado-subencargado-21-03-2012.pdf.

[7] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp214_en.pdf.

Developing GDPR certifications for purposes of data transfers should be a strategic priority for the Commission and/or the EDPB. Certifications can be used as accountable, safe and efficient cross-border transfer mechanisms under the GDPR provided they are coupled with binding and enforceable commitments, including with regard to individual rights. The effect of a GDPR certification as a cross-border transfer mechanism could be even stronger when the certification is made interoperable with other similar mechanisms. It is imperative that this be taken into account when developing certifications to ensure the extension of their geographic cover and reach. Certifications based on the EU-US Privacy Shield and the APEC CBPR are of particular importance in this context. Unnecessary proliferation of different certification schemes should be avoided and GDPR certifications should aim to harmonise, consolidate and make interoperable existing mechanisms where possible.

The WP29 on 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[8] specify data transfer across borders outside the European Union as a criterion for determining high-risk processing and requiring a DPIA. CIPL believes such an interpretation is problematic because:

- Recital 116 dealing with transfers only refers to "increased risk", which is different from "high risk", and any "increased risk" associated with cross-border transfers, according to this Recital, should be mitigated by the DPAs and the Commission through relevant cooperation structures with their foreign counterparts.

- Under the GDPR, as long as the provisions of Chapter 5 are complied with by companies, transfers outside the EU should be possible without also requiring DPIAs based on the mere fact of transfer. Article 44 is clear in this respect when it provides that "all provisions in this chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this regulation is not undermined". Thus, compliance with all applicable Chapter 5 transfer requirements should eliminate any concerns that the transfers at issue themselves impose "high risks".

- None of the articles of Chapter 5 mention the need to perform any DPIA or the notion of high risk.

As a result, clarity should be provided that international data transfers should not constitute a criterion for high-risk processing if conducted under Chapter 5 requirements of the GDPR.

If you would like to discuss any of these comments or require additional information, please contact Bojana Bellamy, bbellamy@hunton.com, Markus Heyder, mheyder@hunton.com or Sam Grogan, sgrogan@hunton.com.

[8] http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

ANNEX