Centre for Information Policy Leadership
Hunton & Williams LLP

19 October 2017

CENTRE FOR INFORMATION POLICY LEADERSHIP RESPONSE

CONSULTATION BY THE COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS 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 Commission Nationale de l'Informatique et des Libertés (CNIL) on its consultation on transparency and international data transfers under the GDPR.

This response addresses a selection of questions, on which the CNIL 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 and knowledge of 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: How to inform in a clear and comprehensive manner? How can we provide people with information in a way that is clear, understandable and comprehensive? Do you think it is appropriate to standardise the information? How do you think we should prioritise the information? Do you measure the satisfaction of people on the information provided?

Answer:

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); and

– 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.

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.

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

[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.

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 2: Which icons to facilitate immediate understanding of information? What do you think about the use of standardised icons to facilitate transparency? Have you examples? What information do these icons highlight? What are the advantages? The disadvantages?

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: Other matters concerning transparency. Tell us about your questions regarding interpretation or any other issues or feedback regarding transparency?

Answer:

Please see CIPL's white paper on Recommendations for Implementing Transparency, Consent and Legitimate Interest attached as an Annex to this submission.

<u>International Data Transfers</u>

Question 1: The Tools for Supporting Transfers Outside of the EU: For Who? Why? The GDPR now provides a renewed and diversified toolkit for international data transfers (BCR Certifications, Codes of Conduct, etc.). In practice, which tool best suits your needs?

Answer:

CIPL believes that all cross-border transfer mechanisms are of importance and suit different organisational needs depending on the transfer involved. As a result all transfer mechanisms should be developed.

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. There are several areas for further development of SCC:

- 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.

- SCC will have to be brought into 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 these contracts up to date in a quick time frame 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.

It is important to note that there are 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 the Privacy Shield (covering only transfers to the United States) and the administrative burdens of the BCR approval process. Given this reality, it will be important for organisations to educate themselves on other transfer mechanisms available to ensure the uninterrupted continuation of their business operations.

Binding Corporate Rules (BCR): BCR are suited to transferring personal data across corporate groups based on EU data privacy requirements and are binding on all relevant entities and personnel within the group. 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. Areas for further development regarding BCR include:

- Streamlining and improving the BCR system to facilitate faster processing time. 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;

- Allowing companies to leverage their BCR and "upgrade" them to GDPR certification under Article 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;

- Providing BCR-approved companies with a special "fast track" process of updating their BCR in line with the GDPR and future GDPR certifications. BCR-approved companies that update their BCR to be in compliance with the GDPR should not be required to go through another comprehensive review and reapproval process;

- 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:

  - 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.

  - 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.

- 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.

Certifications: 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. Areas for development regarding certifications include:

- Ensuring there are sufficient incentives 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.

- Making the certification scalable and affordable, for all sizes and types of organisations.

- Developing certifications and codes of conduct at EU level so that they are functional and operational in all EU member states.

- Regarding certifications only, facilitating 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 United States, CBPR certification in APEC and BCR in Europe.

Other Mechanisms: Other transfer mechanisms such as consent, adequacy decisions and white lists as well as self-certification arrangements are also suitable mechanisms for cross-border transfers in certain cases. These should continue to be utilised by companies where appropriate and further developed and refined when necessary.

Question 2: BCR: A demonstrator of compliance with the GDPR? Do you view BCR as a compliance tool or simply a transfer tool? Should they be part of a groupwide comprehensive data protection policy? Should they also be the vehicle for this global policy? Have you identified any obstacles to BCR adoption by your group?

Answer:

CIPL views BCR as a transfer tool, a compliance tool and an accountability tool. Corporate rules are a transfer tool as they facilitate the transfer of personal data across a corporate group. However, they should not be viewed exclusively as a transfer mechanism. BCR also act as a compliance tool and are, in essence, an accountability mechanism as they require a comprehensive privacy program and compliance structure, including governance mechanisms, data protection officers (DPOs), policies and procedures, training and communication, audits and assessments and, in general, follow the essential elements of accountability and corporate compliance programs.

The process of obtaining a BCR is rigorous and not one of self-assessment, so without a robust data protection program, BCR approval cannot be achieved. The Article 29 Working Party has previously acknowledged BCR as reflective of the accountability principle.[6] Additionally BCR for processors should serve to demonstrate high levels of compliance by processors as required under Article 28 of the GDPR.

Potential obstacles to GDPR adoption include:

- The lengthy approval process (see recommendations to streamline and improve the BCR system to facilitate faster processing time in question 1 above); and

- Post-Brexit, it will be 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.

Question 5: Certification for International Transfers: What are the advantages? What are the limits? What are the constraints? What are the advantages/disadvantages of certification as a transfer tool? What should be the tools the WP29 should elaborate on to ensure the development of certification as a transfer tool?

Answer:

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.

Question 6: Other matters concerning transfers. Tell us about your questions regarding interpretation or any other issues or feedback regarding transfers?

Answer:

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

[6] Article 29 Working Party Opinion 3/2010 on the principle of accountability, 13 July 2010, at pg. 7.

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 1 of this response (See page 8).

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[7] and the Working Document 01/2014 on Draft Ad Hoc Contractual Clauses "EU data processor to non-EU sub-processor"[8]).

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.).

Additionally, please see CIPL's white papers on Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms and Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy, both of which are attached as an Annex to this submission.

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.

[7] https://www.agpd.es/portalwebAGPD/resoluciones/autorizacion_transf/common/pdfs/MODELO-DEFINITIVO-AEPD_Contrato-encargado-subencargado-21-03-2012.pdf.
[8] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp214_en.pdf.

ANNEX

Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR

Centre for Information Policy Leadership GDPR Implementation Project
19 May 2017

CIPL's TOP TEN MESSAGES ON THE PRINCIPLES OF TRANSPARENCY, CONSENT AND LEGITIMATE INTEREST

1. **Transparency is intended to be user-centric and should not primarily envisage legal compliance.**

2. **Transparency should be context-specific, benefit from the possibilities of new technologies and avoid information overload.**

3. **Transparency should be provided contextually by different methods and at different appropriate times throughout the lifecycle of processing operations.**

4. **Algorithmic transparency should focus on the broad logic involved instead of attempting full transparency to the individual. Most important may be transparency about the inputs to which algorithms are applied.**

5. **Consent should be used as a legal ground for processing in situations where it is possible to provide clear and understandable information at the right time and individuals have a genuine choice concerning the use of their personal data.**

6. **Member states should take a harmonised approach vis-à-vis the age of consent for children. The age should be 13. The practical difficulties and privacy issues arising from seeking to verify parental/guardian rights over the child must be recognised.**

7. **There are concerns about the predominance of consent in the ePrivacy rules. The EU legislator should introduce legitimate interest into the ePrivacy Regulation.**

8. **Legitimate interest may be the most accountable ground for processing in many contexts, as it requires an assessment and balancing of the risks and benefits of processing for organisations, individuals and society.**

9. **Legitimate interest places the burden of protecting individuals on the organisation, which is in the best position to undertake a risk/benefits analysis and to devise appropriate mitigations.**

10. **The legitimate interests to be considered may include the interests of the controller, other controller(s), groups of individuals and society as a whole.**

1. INTRODUCTION

1.1 The GDPR requirements on transparency, consent and legitimate interest

The GDPR recognises transparency as a core principle of data protection. Transparency is related to the fair processing principle. Processing can be fair only if it takes place in a transparent manner.

However, transparency can serve its purpose only if it is meaningful. There currently is a growing gap between legal transparency and user-centric transparency. Concise and intelligible privacy notices focusing on truly informing users by providing meaningful information are at the center of user-centric transparency.

Transparency in the GDPR is intended to be user-centric. It should be an effective instrument for the empowerment of the individual, one of the main objectives of the GDPR. This is why CIPL's recommendations focus on user-centric transparency. Transparency should be context-specific, flexible, dynamic and adaptable to constantly evolving and changing uses to provide clear and understandable information to individuals and to enable a genuine choice where it is possible about the use of their personal data. However, even where consent is not available, transparency is still necessary to provide relevant information about the processing activities, how the organisation has mitigated the risks, the rights of individuals and any other relevant information demonstrating that the organisation is fully accountable for its processing activities.

Further, in situations where consent is deemed impractical or ineffective and does not appear to be the most appropriate legal basis, if only because of the complexity of modern information uses, other legal bases, including the legitimate interest ground for data processing,[1] can be relied upon. Legitimate interest requires an assessment and balancing of the risks and benefits of processing for organisations, individuals and society. It also requires the implementation of appropriate mitigations to reduce or eliminate any unreasonable risks. This places the burden of protecting individuals on the organisation and shifts it away from individuals. Organisations are in the best position to undertake a risk/benefits analysis and to devise appropriate mitigations, and individuals should not be overburdened with making these assessments and informed choices for all digital interactions and processing of their personal data.

1.2 The CIPL GDPR Project

This paper by the Centre for Information Policy Leadership at Hunton & Williams LLP ("CIPL")[2] is a part of its project on the consistent interpretation and implementation of the GDPR ("CIPL GDPR Project").

The CIPL GDPR Project—a multiyear project launched in March 2016—aims to establish a forum for dialogue amongst industry representatives, the EU DPAs, the European Data Protection Supervisor, the European Commission, the ministries of the member states and academics, on the consistent

[1] There are additional grounds for processing (e.g. contractual necessity) not discussed in this paper but also applicable in many circumstances and important for organisations as a legal basis for processing.

[2] CIPL is a privacy and data protection think tank in the law firm of Hunton & Williams LLP and is financially supported by the law firm and more than 50 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 to ensure effective privacy protections and the effective and responsible use of personal information in the modern information age. For more information, please see the 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 Hunton & Williams.

interpretation and implementation of the GDPR through a series of workshops, webinars, white papers and comments.

CIPL aims to provide input to the Article 29 Working Party ("WP29") on a number of priority areas, identified in CIPL's GDPR Project work plans for 2016 and 2017. This is the fifth white paper in this series, following earlier CIPL papers on DPO, Risk, OSS and Lead Authority, and Certifications.[3] CIPL also submitted comments to the WP29 on its Guidelines on the right of data portability, OSS, Lead Authority and the DPO and DPIAs and "high risk".[4]

1.3 CIPL's White Paper

In this white paper, CIPL aims to provide the WP29 and data privacy practitioners with input on transparency, consent and legitimate interest—three core concepts of the GDPR. Accordingly, the paper sets forth CIPL's recommendations on how to apply and implement these concepts. It also notes certain open questions that might be further explored. The relevant GDPR provisions on each of these items are summarised at the end of this paper.

The items were discussed during a workshop organised by CIPL in Madrid on 7 March 2017. The input received at the occasion of this workshop is taken into account in this paper.

[3] See
https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_gdpr_dpo_paper_17_november_2016.pdf;
https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_the_gdpr_one-stop-shop_30_november_2016.pdf;
https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.
PM.

[4] Available on www.informationpolicycentre.com.

2. TRANSPARENCY

2.1 Starting points

- **Transparency is key to ensuring that processing is fair.** The GDPR firmly links transparency to fair processing. It states in its first principle that personal data must be "processed lawfully, fairly and in a transparent manner".[5]

- **Transparency is a business consideration and priority**. It is critical for trust and digital confidence, and goes beyond pure legal compliance. By effectively informing individuals about the protection and use of their personal data, including benefits of data processing, and by addressing the concerns of regulators, transparency will have the effect of raising the level of digital education, broadening individuals' expectations, increasing their acceptance of and support for certain data uses, and generally deepening individuals' and regulator trust. This in turn will enable organisations to use data for wider and more beneficial purposes, and also encourage competition around the most effective transparency. All of this benefits individuals, organisations, society and the Digital Single Market.

- **Transparency in the GDPR is broader than privacy notices** provided at the time of data collection and privacy policies provided in general on organisations' websites. Transparency includes all mechanisms and instances used by organisations to communicate with an individual. For example, transparency also includes product and service descriptions that explain how personal data will be used, communications in respect of the exercise of individuals' rights and notification to individuals of data breaches.

- **Effective transparency requires a new multidisciplinary approach, innovative delivery and tools, and robust resourcing and investment.**

2.2 Transparency delivers effective compliance with other GDPR requirements

- **Transparency will have a role in defining and supporting the purposes for which personal data may be used** (including compatible uses for further processing), as well as for specifying the grounds for processing.

- **Transparency is an intrinsic part of any consent**, as consent must be informed in order to be valid. Transparency concerning the uses (including unexpected and future uses) of data, the benefits of processing and the organisation's accountability measures are all important to enable individuals to make choices.

- **Privacy notices of Articles 13 and 14 must be provided, irrespective of the ground for processing.** Transparency also offers benefits to the individual in situations where individuals do not have a choice on data use, or where consent is not feasible, impracticable or ineffective and/or where other legal bases are used. Transparency requires that organisations should be transparent about the data uses based on a legitimate interest ground. It is also important in respect of the legal basis for contractual necessity, by precisely defining the services within the contract.

- **Transparency has a role in setting the reasonable expectations of individuals** regarding the use of their personal data. For example, in the context of legitimate interest processing, the

[5] Art. 5 (1) GDPR. Indeed, fair processing is at the core of EU data protection. See also Art. 8 of the EU Charter on Fundamental Rights.

reasonable expectations of the individual are one element that a controller must take into account as part of the legitimate interest balancing test. Transparency and notices to individuals can shape the expectations of individuals as to how their personal information might be used.

2.3 Transparency as an element of organisational accountability

- **Transparency is an essential element of accountability.** Together with other accountability elements, transparency ensures responsible data use.

- **Transparency is complemented by other accountability elements, such as risk assessments, data protection management (e.g. DPO, CPO) and individual rights (access, portability, correction, objection).** Sometimes, organisations without a direct relationship with individuals will need to rely on other mechanisms to ensure they are fulfilling their accountability obligations and to compensate for the possibility that it will be challenging to fully satisfy all transparency requirements. Under those circumstances, these other accountability measures become important for delivering effective data protection for individuals and ensure responsible data use.

2.4 User-centric transparency is key

- **There is a perceived growing gap between legal transparency and user-centric transparency**. Legal transparency, T&Cs and privacy notices are necessary to comply with data protection law, but arguably they do not always effectively deliver transparency or understanding to individuals. In fact, perhaps the reverse is true, as they must follow specific legal mandates. This is even more complicated where the organisation operates in multiple jurisdictions and must try to tailor legal notices to numerous and sometimes competing legal requirements. User-centric transparency is about delivering transparency as part of the customer relationship and digital trust. It is also about building understanding and explaining the benefits of data use and the value of the product or service, organisational accountability, and the choices that are available.

- 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 and the requirement that notices be clear and concise. Thus, where the goal is to provide understandable and actionable information to individuals, it may be challenging to systematically communicate every complex detail. **There needs to be an effort to find a balance between clarity and completeness and to resolve this balance in favour of clarity through innovative ways of delivering required content of notices.**

- **GDPR transparency is intended to be user-centric.** This is why Article 12(1) GDPR requires that information is provided to the individual in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

- **Transparency should be designed to effectively provide relevant, timely and digestible information** to individuals when and where it is most meaningful to them. This can be done both based on the “push” model (proactively providing just-in-time transparency) and the “pull” model (making information available to individuals at their convenience, e.g. permission management, transparency dashboards and “learn more” tutorials).

- **The possibilities of a pull model should be further explored** to allow provision of information to individuals who desire it. Some information must always be provided under

the GDPR, but that should be the most important information to enable choices or deliver user-centric transparency. The rest should be made available to individuals in an accessible location or manner. This approach is also in line with the layered notices approach.

- **Transparency should be driven** not only by the legal requirements but also **by the real needs**, **interests and concerns of individuals** with respect to data processing. These can be determined through researching and testing how people actually interact with services and what concerns they may have about the use of data.

- Organisations face **real practical challenges in complying with the strict letter of Articles 13 and 14** for every single processing purpose of data in the modern digital economy and society. Hence, it may be better for both organisations and DPAs to focus on achieving real and user-centric transparency that remains true to the spirit and objective of the law and that is more effective in protecting individuals and their data than the lengthy and legalistic privacy notices and policies that would follow from the strict interpretation of Articles 13 and 14.

- In practice, **transparency may have to be delivered by (a) actionable and targeted user-facing information** focused on individuals and their needs; **and (b) more detailed legal disclosures** (privacy notices and policies) that are designed to ensure legal compliance as well as to provide comprehensive and accountable information for those who seek it (general public, NGOs, DPAs), in a manner that remains as clear and concise as possible.

2.5 Specificity of and exemption from notices

- **Transparency means that organisations need to provide the following key information** in a concise and intelligible manner: a) all purposes of processing; b) reliance on the legitimate interest processing ground; c) the logic in automated decision making; d) use of third parties to process data; e) cross-border data transfers; f) data retention period; and g) individuals' rights (access, rectification, objection, etc.).

- It should be acceptable to **provide the full list of required elements of a privacy notice under Articles 13 and 14 in a generic privacy policy**, instead of providing this notice for each single collection and use of data. Presenting all this information to users at the time of collection will only undermine the very transparency the GDPR is seeking to achieve by overwhelming a user with information that in many cases they simply do not wish to actively consume.

- **Specific or just-in-time privacy notices** should be reserved for actionable information and limited to cases where provision of such privacy notices is warranted, such as where there is a higher risk of processing, or where there are unexpected uses of data, or in cases of sharing with third parties that is outside the normal provision of the services. Also, these methods are generally more applicable and viable for the online and mobile environment, and where there is real-time interaction (online or call-centre situations, for example).

- It must be possible for a controller to **rely in certain cases on the exception for disproportionate effort (Art. 14(5))** as an exemption to providing notice under Article 14. Moreover, this exemption must be possible of being interpreted broadly, especially where organisations do not have direct relations with the individuals and in cases where the provision of a notice would prejudice the very purpose of processing and the legitimate rights of organisations and other parties (e.g. fraud prevention, information and system security, corporate investigations).

2.6 Gap between industry practices and understanding of consumers

- **Transparency must go hand in hand with broader consumer education and digital literacy initiatives**. This is essential to address the growing gap between the technology and business processes on the one hand and the general understanding of the public about data uses and the digital ecosystem on the other. This is the responsibility not only of organisations using data and technology, but also of the media, the DPAs, NGOs and other relevant organisations. It is part of the task of the DPAs to promote public awareness (Article 57(1)(b) GDPR).

2.7 Transparency where there is no direct relationship with individuals

- Transparency is increasingly difficult in complex data ecosystems where organisations do not have a direct relationship with individuals, or where they just process pseudonymous data and do not have the ability to identify individuals themselves.

- Where data is **pseudonymised** or relates to individuals who cannot be identified from the information in the possession of the organisation, **organisations should not obtain additional data in order to provide a data privacy notice** to such individuals, or to answer an access/portability/erasure request with respect to them. This raises questions about the definition of pseudonymisation and how the GDPR requirements apply to these data categories.

- There should be **flexibility in interpreting** the requirement of transparency in practice and in addressing the above challenges, especially **the strict and long list of requirements of data privacy notices in Articles 13 and 14**. The interpretation should allow for more creative and distributed ways of providing necessary information to individuals.

2.8 Algorithmic transparency should be focused on the broad logic involved

Algorithmic transparency vis-à-vis individuals and the general public must be achieved in a manner that is realistic and effective in practice. As the GDPR recognises, there is no obligation to provide detailed information about the algorithm itself, merely the logic behind it. Individuals will not have the time or inclination, and most likely not the ability, to understand the algorithms behind big data and machine learning applications. To illustrate the issue: individuals rely on brakes in cars without understanding how they work. However, there is certainly a place for regulators to understand brakes. It should be the same with algorithms and data processing—algorithmic transparency may be more appropriate vis-à-vis DPAs in connection with their oversight and enforcement roles.

Algorithms are not static and defy real-time explanation. To complicate things further, algorithms cannot be understood in a static manner. It is inherent in all algorithms and machine learning techniques that they constantly change based on accumulated knowledge and insights. This makes it difficult to deliver real-time and detailed transparency on the workings of algorithms.

- **Focus on objectives and outcomes of algorithmic transparency.** Providing the "logic behind" algorithms means that there is an obligation to consider the intended objectives of algorithmic transparency vis-à-vis individuals, and then deliver the desired outcomes through appropriate means.

- **Algorithmic transparency should be focused on the broad logic involved** and not the detailed workings of algorithms. A key element **is to be transparent about the type of inputs to which algorithms are applied as well as on the outputs, and to ensure that they are both accurate and correctible.**

- **Other internal accountability mechanisms and tools are essential.** This includes DPOs who exercise oversight and advice in respect of the use of algorithms and machine learning. Accountability should also include the safeguards, as articulated in Article 22 GDPR. Also, as mentioned above, more details concerning algorithmic transparency may be part of transparency vis-à-vis DPAs in the event of a complaint, investigation and enforcement action or on request, respecting the confidentiality of trade secrets.

- **GDPR certification could be a useful instrument to increase transparency of algorithms.** Certification does not necessarily increase transparency of algorithms to individuals directly, because the GDPR provisions on certification[6] only require transparency to a DPA or a certification body. However, certification can provide assurances to individuals that a DPA or a certification body has reviewed and approved the processing at issue.

2.9 Limitations on transparency

- **Transparency cannot be absolute.** Transparency is an essential element of effective data protection, but is subject to limitations imposed by the complexities of the modern digital economy and the other rights and freedoms. This must be recognised. There should be a number of factors that define the limits.

- Transparency **may be limited by trade secrets, commercial and competition considerations, other intellectual property rights, as well as by rights of other individuals.** Equally, there may be cases where full transparency to individuals may be inconsistent with public interest considerations and prejudice organisations' ability to conduct essential and common data processing, such as fraud prevention, or corporate investigations, or to implement information and network security measures.

2.10 Contextual means for delivering transparency

- **The means of delivering transparency and its content must be contextual and allow for appropriate discretion to organisations.** Transparency must take into account the nature of services being provided and the relationship between the organisation and its customers/individuals. It must give individuals understanding and clarity about the products and services they are obtaining and the use of their personal data in that context.

- **Transparency must be provided by different methods and at different appropriate times throughout the lifecycle of the data** and the related products or services used by the individual. Transparency should make it possible to understand the processing of personal data *ex ante* and *ex post,* enabling individuals to exercise their rights at the appropriate time. One way to provide ongoing transparency and control would be periodic reminders about data and privacy settings, while also retaining the organisation's flexibility to adjust to the specificities of a given service, circumstance and user expectation.

- **Transparency mechanisms and tools must change with and adapt to technological changes.** They should not be too technology specific, stifling innovation.

[6] In particular Article 42 GDPR.

- **Transparency mechanisms must be embedded as much as possible within the relevant product, service, process or technology.** They should not be at the expense of usability and functionality of any given technology or create burdens for individuals as they use technology in their daily lives and work.

- Effective mechanisms for transparency may include **push and pull mechanisms**, and can be delivered via a combination of tools, such as privacy policies, layered notices, just-in-time notices for websites, dashboards, control panels, custom-built apps, tutorials, user guides, interfaces, etc.

2.11 Icons: not in all cases and not top down

- Standardised icons are presented in Article 12(7) of the GDPR as a specific transparency tool and the Commission is empowered to adopt delegated acts to specify the use of this tool.

- **The feasibility of employing icons** and standardised policies as effective transparency mechanisms should be based on research and evidence. The views and experiences of privacy practitioners and experts regarding their usefulness are split, ranging from extremely skeptical to somewhat optimistic in limited contexts.

- Icons might be able to provide useful information and create market value in some cases, but they are also considered to be static and thus inappropriate for modern ways of processing data that are constantly evolving with innovation and cannot be captured by simplistic and fixed icons. Icons represent the state of play at a certain moment and do not take account of changes in technology and business practices. Also, if there are too many icons, they will not simplify or promote user-centric transparency for individuals. Instead, having to learn icons may be perceived as burdensome.

- For **icons** to be useful, they **should not be created and imposed "top down".** To the extent possible, they should be developed initially by industry and then vetted, refined and potentially harmonised in collaborative stakeholder processes. However, organisations must also have the flexibility to create and deploy their own icons to suit their brand, products and services.

- **Encourage harmonisation, not standardisation.** Icons should not be standardised across different subject matters and applications, suiting all categories of individuals (customers, employees, citizens) and all different data uses and alternative platforms. However, harmonisation should be encouraged so as to avoid confusion of individuals having to learn the differences between different icon systems.

- **Interactive tools are in many cases a better alternative**. Rather than force users to understand icons, we should develop transparency technology that understands the user and that reacts to the user. Examples are user-friendly chatboxes or chatbots. Machine-learning should play a role; human interfaces should also play role.

2.12 Develop effective transparency tools by multidisciplinary teams

- Organisations will be the ones that will have the best sense of what may work and the individuals they interact with may be best placed to determine how any transparency tools may fit into user interfaces, experiences and the organisation's brand and design standards.

- The most successful transparency tools and methodologies will be those not built only by lawyers, but that are built **by multiskilled/multidisciplinary teams** that include behavioral economists, user interface and design scientists who are expert in human factors or ergonomics, social scientists, psychologists, technologists and communication experts. DPAs could be included in the process as well at their own discretion.

2.13 Transparency and DPAs

- **Accountability** includes the obligation to demonstrate compliance, which by definition **requires some transparency to DPAs**. Transparency vis-à-vis DPAs is also an objective of consultations between businesses and DPAs and of responding to information requests in the context of regulatory oversight matters and investigations.

- **DPAs should recognise organisations that have developed innovative and effective user-centric transparency as accountable organisations**. Positive and reinforcing messages and showcasing "what the good looks like" by DPAs can be a way to deliver such recognition, in addition to the methods mentioned below.

- **DPAs should incentivise diverse user-centric transparency and showcase best practices**. They should not impose on organisations one-size-fits-all solutions and tools, but take into account differences between industry sectors and user expectations.

- DPAs may also incentivise and recognise transparency by giving **significant weight to effective and user-centric transparency in investigations and enforcement actions**.

- **Enforcement by the DPAs** should **not** be based primarily **on failure to comply with the precise letter of Articles 13 and 14**, but rather on how effective organisations are in delivering user-centric transparency.

3. CONSENT

3.1 Starting points

- **The GDPR places all processing grounds on an equal footing.** Consent is one of the grounds for processing personal data in the GDPR. It is neither the only ground nor the most important one.[7]

- **Consent should be used as a legal ground for processing where:** a) it is possible to provide clear and understandable information; b) individuals have a genuine choice to decide whether to use a service or not; and c) consent can be withdrawn without any detriment to individuals (although this may result in inability to use a service). Organisations should not be expected to offer a "shadow service" without personal data if the very service itself relies on personal data to provide the very best user experience.

- **Overreliance on consent undermines its quality and creates consent fatigue.** Overreliance on consent or use of consent in contexts other than the situations described above will undermine the quality of the consents that are obtained. Equally, it will not achieve the

[7] Art. 4(11) GDPR defines consent as: "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

desired purpose of putting individuals in control, but instead create a consent fatigue with people using services and technology in their daily life and work.[8]

- **Other processing grounds may be more appropriate in some instances.** In many situations it may, for a variety of reasons, be more appropriate for organisations to use other legal grounds for processing, such as legitimate interest, necessity for fulfilling a contract or a legal obligation. If individuals do not have a real choice, or cannot be provided the necessary information as a result of the complexity of modern data uses, or if the withdrawal of consent is not possible for the organisation, legitimate interest or contractual necessity may be the most appropriate or most effective and accountable tool for protecting individuals.

3.2 Consent iscontext-specific and must be adapted to the information society

- The implementation of consent should align with the underlying policy goals behind consent: (a) **individuals have the information they need to make informed choices** about their data; (b) **individuals can make those choices before their personal data is being processed**; and (c) **individuals can withdraw their consent any time thereafter but should understand that this may mean that a specific service may no longer be offered**.

- **The GDPR sets out some new requirements for valid consent**. Not only must consent be informed, specific and freely given, but the GDPR also requires consent to be a) distinguishable from other terms and conditions; b) separate for each processing operation; c) not conditional on the performance of a contract; d) not used in situations of clear imbalance of relationship between the organisation and individuals, e.g. in an employment relationship; and e) able to be withdrawn at any time. This will require organisations to consider carefully how to organise and deliver consent in a way that is appropriate for the circumstances, does not overburden individuals and creates legal certainty to allow them to rely on consent.

- **The implementation of consent must be adapted to the modern information age.** This is not only because of the complexities and volume of data processing, but also because of the effect on individuals of actively providing consent as they interact with technology in every aspect of their lives and their work. Individuals will not expect to have to legitimise every single use of data, or every single processing operation, technology and the provision of products and services they want to use. In fact, individuals will expect organisations to use data and develop products, services and technology in a responsible manner and to use consent as a means to legitimise data use in situations where there is a clear and easy choice for individuals.

- **Normally, the GDPR does not require "explicit consent" and organisations have flexibility in how they obtain consent in accordance with Article 7 GDPR. Thus, clear affirmative action or statements as modalities of consent should be interpreted flexibly.** The validity of consent mechanisms should be examined in context, avoiding strict or static interpretations of consent requirements and evaluating consent flows based on user expectations in a given situation. There will be circumstances where a valid consent will be given by a clear

[8] This is also the practical approach taken by industry, as confirmed by the recent CIPL and AvePoint GDPR Readiness Survey Report. Some organisations heavily rely on consent today. Under the GDPR, they will continue to use consent in situations where organisations are able to obtain valid consent, or where local law imposes a consent requirement.

affirmative action that indicates the individual's agreement with the use of personal data. For instance, when an individual fills out an online form provided by a service provider, he consents to the use of his personal data in relation to the requested service by submitting the completed form. Another example of a consent by an affirmative action is a request of an individual for an individualised service, or an employee who has a choice to take part in her company's diversity survey and after a full notice about the use of her data clicks the link to take the survey. This consent extends to all processing reasonably related to this service, or the survey, as stated in the notice.

- **Explicit consent is only required for certain processing.** Explicit consent is a higher and stricter level of consent required by the GDPR for processing of special categories of data, automated decision taking where there is a legal effect/similarly significant effect, and as a derogation for the international data transfers prohibition. Explicit consent means that an individual states that he or she agrees with a specific use of his or her personal data, which requires such heightened consent.[9]

- **Further consideration is needed on contextual ways to express and revoke consent** under the GDPR. Especially, a) the provision of consent by "affirmative action" (e.g. recognising the completion of the online form explained above); b) an interpretation of the meaning of "revoke consent in the manner given"; and c) the relationship between the "right to object" and withdrawal of consent. CIPL recommends a flexible interpretation of points a) and b) above. Revoking or withdrawal of consent can certainly be made in multiple ways, depending on circumstances. For example, an individual who provides oral consent over the phone should be able to revoke consent on an online dashboard or a permission management portal/app at a later time. At a minimum, organisations should be able to satisfy the obligation to provide withdrawal of consent by offering individuals the ability to terminate their relationship with the organisation.

- **The notion of compatible use should be interpreted to include further processing of personal data that benefits the common good and society and does not create risks and harms for the individual**. There is a link between consent and further processing for compatible purposes. "Compatible" future uses or new uses do not require a new legal ground but may require organisations to provide notice to the individual in some cases. So-called incompatible future uses or new uses of personal data require a new legal ground for processing, such as consent. It is essential that in an information society and in the context of Digital Single Market the notion of compatible use is not interpreted in such a limited manner that it impacts or impedes the ability of organisations to engage in beneficial new data uses and data innovation, especially where these further data uses do not create risks and harms for individuals. In these situations, a new consent should not be required. Furthermore, any future use that does not undermine, contradict or in any way interfere with, or that can coexist with, the original use is, by definition, "compatible" with the original use within the common meaning of the word "compatible". Obviously, data sets that are de-identified or anonymised fall outside the scope of the definition of personal data and can be used for further and different purposes.

[9] The interpretation of explicit consent under the GDPR should not depart from that of Directive 95/46/EC, which also requests explicit consent for processing of special categories of data. Oral explicit consent is not excluded.

- **Pre-GDPR consents should continue to be valid if they have been obtained in compliance with the Directive and national law.** Organisations should not have to re-paper existing consent until there is a material change in processing and its purposes. The only exception are cases where existing consents do not comply with the GDPR's requirement that performance of a contract or service is not conditioned on consent to processing that is not necessary for the performance of a contract or, in connection with a child, the requirements of Article 8(1) have not been met.[10]

- **The GDPR consent should accommodate product development.** In some instances, certain data processing may be required to provide new features or functionality of a service or a product, and a user may need to decline to use the product if they do not want their data processed in that way.

  The concept of freely given consent under Article 7(4) should be interpreted to accommodate processing for product development, so that in instances where consent is required, there is no obligation to continue to support static, outdated versions of products if users do not wish to provide consent. The GDPR should not artificially constrain launching new functionality for users.

3.3 Contexts where other legal bases may be more appropriate than consent

While consent has a role to play in data protection law and practice, CIPL believes that in many situations other data protection concepts and tools may be more appropriate. Indeed, in cases where consent may not be available, there are other tools that can protect the individual. The examples of such tools and concepts empowering the individual and ensuring focus on the individual are: transparency, risk assessments, legitimate interest, organisational accountability, data protection by design, security measures, exercise of individuals' rights, redress in case of an infringement, etc.

3.4 Children's consent should be valid from the age of 13

- **Member states should take a harmonised approach to the age of consent for children** to enable delivery of the same digital services, products and technologies across the EU. Differences of minimum age would create obstacles for seamless development and delivery of service across the EU, prejudice the functioning of the Digital Single Market and may also complicate the control by DPAs and their cooperation. Moreover, there is no reason why in some EU member states children should be treated differently than in others.

- Member states should be encouraged to provide through national law for **the age of consent at 13**. This is consistent with the latest research.[11] Any higher age of consent would prejudice the children's right to privacy and data protection, as their participation in the information society would be subject to parental knowledge and consent.

- **It should not be required under the GDPR to collect unreasonable amounts of additional information to verify parental/guardian rights over the child, or to verify the age of the**

[10] This is consistent with the September 2016 opinion of the German DPAs of the Duesseldorfer Kreis.

[11] See Janet Richardson, et al., "EU General Data Protection Regulation: teen access to internet services; 5 reasons why they shouldn't require parental consent above age 13", 3 March 2017, available at https://medium.com/@janice_richie/eu-general-data-protection-regulation-teen-access-to-internet-services-685cbef7aeab.

children. "Reasonable efforts" to confirm that the person consenting is a person holding parental responsibility would be sufficient. This approach would be in line with the regime in the United States under the Children's Online Privacy Protection Act (COPPA), which requires only that methods used to obtain verifiable parental consent be reasonably calculated in light of available technology to ensure that the person providing consent is the child's parent. This does not require organisations to collect additional information above and beyond the approved methods of parental consent, which serve as proxies for parental verification. Use of readily available consumer technologies, such as credit card transactions, should be allowed, and new technologies should be supported provided they meet the standard.

- **Further discussion is needed on how to best implement the children's consent requirements.** This would include analysis and development of best practices around consent verification, among other issues, based on relevant experience under COPPA. CIPL offers to facilitate such multistakeholder discussions to study these issues further.

3.5 Concerns about the predominance of consent in the ePrivacy Regulation

- **The proposed ePrivacy Regulation may have unintended consequences of undermining the application of the GDPR by requiring consent in a wide range of situations,** relating to electronic communications content or metadata, as well as the information stored in and related to terminal equipment. The proposal extends to all communications, including machine to machine and IoT outside the traditional telecommunications sector. Activities that would be legal under the GDPR would be made illegal because of the broad application of the ePrivacy Regulation and its strict consent requirements.

- **The ePrivacy Regulation risks undermining the usefulness/availability of other processing grounds, especially the legitimate interest processing ground in the GDPR**. As explained, the legitimate interest processing ground may in many situations be more appropriate. One should avoid any unintended consequence of excluding many new and future uses of electronic communication data (including metadata and content), which may be perfectly legitimate, customary and safe for individuals in the digital economy.

- The proposed ePrivacy Regulation is the subject of a forthcoming CIPL discussion paper which will be very critical about the heavy reliance on consent to the exclusion of other grounds for processing, highlighting not only the negative impact for individuals to benefit from data uses, but also the risks to the protection of their personal data. The paper will provide suggestions for limiting the scope of application of the ePrivacy rules and for **introducing the concept of legitimate interest into the ePrivacy Regulation** to align it more with the GDPR, possibly in combination with a risk-based approach.

- **The application and interpretation of consent under the GDPR and the ePrivacy Directive (and the proposed ePrivacy Regulation) must align.**

4. LEGITIMATE INTEREST

4.1 Starting points

- **Legitimate interest is an essential processing ground in the modern information age**. It ensures that the GDPR remains future-proof and technology neutral. It enables ongoing delivery and improvement of products and services, and new and innovative uses of data,

while ensuring organisational accountability and respecting data protection rights of individuals.

- **Legitimate interest is an element of and supports the controller's accountability.** It must not be considered as a processing ground of last resort. In many instances, it is a more accountable and effective tool for protecting individuals than other grounds, including consent.

- **The WP29 Opinion on legitimate interest of 2014[12] provides a useful and still relevant discussion of legitimate interest**. It provides useful examples and enables an understanding of possible practices of legitimate interest. The annex of this paper elaborates a number of examples of the legitimate interest ground for processing of personal data, based on the practices of the organisations participating in CIPL's GDPR project.

- **A general nonexhaustive "database" of legitimate interest processing cases may facilitate proper implementation of this requirement in the future.** We encourage the establishment of such a database by the EDPB with inputs from a multistakeholder group, including DPAs, industry and civil society.

4.2 Scope

- Legitimate interest is particularly useful because of the broad scope of application of the GDPR. Given this wide scope, **it is not possible to predetermine all contexts or processing activities where the legitimate interest ground may apply**. The basic purpose of the legitimate interest ground is to enable it to be applied contextually in cases where the conditions are right.

- **It is possible to articulate general categories of processing where legitimate interest typically does, or might, apply**. This approach is reflected in GDPR Recital 47 and demonstrated in CIPL's paper on legitimate interest case studies. Examples are: processing of customer or client data, including for direct marketing and advertising more broadly; processing of employee and customer data within a corporate family or group of undertakings for administrative purposes; processing payments/subscriptions to fulfill financial commitments and contracts; processing of data necessary for network and information security, processing for fraud prevention and investigation; certain data transfers.

- **Legitimate interest facilitates low-impact data processing**. Legitimate interest is particularly useful because of the broad scope of application of the GDPR, which includes a wide range of situations of personal data that is collected, used or shared that has little to no impact on the private life of individuals and does not create any risks for individuals. Legitimate interest facilitates the evaluation of this type of processing and the implementation of necessary controls, if any, with respect to this data, thereby enabling use of the data without resort to consent. Appendix II provides useful examples.

- **The legitimate interest to be evaluated may be the commercial or other interests of a controller but also may be the interests of other controller(s), groups of individuals and society as a whole.** Examples of the interests of society include: spam and fraud prevention,

[12] Article 29 Data Protection Working Party, 844/14/EN, WP217, Opinion 06/2014, on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014.

improvements in health provision and prevention, environmental protections, infrastructure, scientific advancement, timely payment processing and invoicing, cybersecurity, tax collection, etc. In that connection, it should be recognised that commercial organisations often work in the public interest and that their own legitimate business interests may also involve benefits to third parties and society.

- **The legitimate interests of the controller or a third party may also include other rights and freedoms.** The balancing test will sometimes also include consideration of other rights and freedoms, such as freedom of expression, right to engage in economic activity, right to ensure protection of IP rights, etc. These rights must also be taken into account when balancing them against the individuals' right to privacy.

- **CIPL proposes to identify and further develop lists of general criteria that can help establish a potential legitimate interest**.

4.3 The limitation for special categories of sensitive data

- **Special categories of data (or sensitive data) may not be processed on the basis of legitimate interest.** This raises problems, particularly in relation to processing in which the controller or processor does not have direct contact with the individual and cannot ask for consent and also given the growing use of biometrics, for security, verification and authentication purposes. Examples include CCTV, or facial recognition by retailers to identify known shoplifters, or use of fingerprints for payment ID.

- **Anonymisation and pseudonymisation could be solutions and should be further developed**. First, anonymisation may resolve the problem in contexts where full anonymisation is possible and subsequent re-identification is not possible or needed. Second, pseudonymisation is an instrument that allows for transforming sensitive data into "ordinary" personal data, representing low risks for the individual. Pseudonymised data may be processed on the basis of the legitimate interest ground, which is particularly attractive in view of the low risk for the individuals after pseudonymisation.

- Pseudonymisation should also be further developed for specific contexts where additional safeguards apply. An example is clinical research where legal, ethical and contractual safeguards must be applied in addition to a very specific codification process.

4.4 The balancing test

- **The legitimate interest ground is no carte blanche for processing.** Instead, the balancing test under legitimate interest requires a context-specific risk/benefit assessment and implementation of potential mitigations as part of organisational accountability.

- **Each controller is responsible to ensure that the application of the legitimate interest ground for a new processing purpose meets the relevant balancing test**. Moreover, each new or changed proposed processing purpose must be reviewed de novo under the legitimate interest balancing test.

- **DPAs should be available and accept informal consultations** when businesses conduct the relevant risk analysis or balancing test.

- **Industrialise risk assessments, but accept that they are context-specific.** The weighing of legitimate interests and benefits of controllers or third parties against competing individual rights and freedoms and the outcomes of risk assessments are **context-specific**. Organisations will have to become proficient in conducting risk assessments in the context of applying the legitimate interest ground.

- However, this **does not preclude a general framework or guidance** that would enable businesses to identify processing activities that are likely to meet the legitimate interest requirements (subject to verification) or to consistently identify/assess potential risks or harms to individuals. The WP29/EDPB should play a role in developing a general framework or guidance on this issue, as a follow-up of the "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".[13]

- Given that **organisations must take into account the reasonable expectations of individuals** in determining the legitimate interest and performing a balancing test, it may be possible to identify generally accepted examples of "reasonably expected" processing, i.e. activities that are customary and reasonable and thus should be "reasonably expected". This should include services where advertising is a normal feature related to the service. In addition, it should be reasonably expected that organisations will analyse their customers' data to make improvements to their products and services or to develop new products and services.

  However, even where a proposed data use was not within the reasonable expectations of a data subject, it should still be possible to rely on the legitimate interest balancing test to authorise that use. While it is essential that organisations take into account the reasonable expectations, the public interest or other factors considered in the balancing test may support an unexpected use.

- **The test for legitimate interest must be flexible.** The "reasonable expectations" of individuals change over time and the legitimate interest balancing test must be capable of taking these changes in reasonable expectations into account.

4.5 Transparency

- The requirement to **provide the legitimate interest pursued by the data processing in privacy notices to individuals must be implemented with flexibility.** DPAs should recognise practical challenges in delivering this information in every single case of legitimate interest processing. Organisations should be allowed to provide general information about the legitimate interests pursued in their privacy policies. In some instances, it may be actually prejudicial to provide a detailed notice about a processing based on legitimate interest, where that may prejudice the purpose of processing, such as in respect of information and system security or fraud prevention processing.

4.6 Legitimate interest and cross-border transfers

[13] Adopted by the WP29 on 4 April 2017. See also CIPL's December 2016 white paper on "Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR", which provides guidance on devising such a framework to identify and assess the risks and benefits associated with processing, including in the context of establishing a legitimate interest ground for processing. See https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.

- **The WP29 should develop guidance (including examples) for use of legitimate interest as a ground for cross-border data transfers**, given the higher threshold for legitimate interest as a basis for data transfers in the GDPR (see Article 49(1)(g). The GDPR refers to notification to individuals and DPAs and to the assessment of all circumstances surrounding the transfer, as additional elements of a legitimate interest test.

- **Legal requirements or legitimate administrative requests for data in non-EU countries should be considered as an example of a legitimate interest enabling data transfers in specific and limited instances.** There are numerous examples, such as a requirement of a third country to give tax authorities of third countries access to personal data, or a need to provide senior leadership data to a foreign client for the purpose of a public service tender, or a requirement to provide data for e-discovery and judicial proceedings purposes, or an export control law requirement to check against economic sanctions lists.

- **International data transfers necessary for global cyber threat intelligence and security should be considered to be based on legitimate interest,** consistent with Recital 49.

Appendix I
Relevant GDPR Provisions

GDPR Transparency Requirements

Transparency is now **explicit requirement** and part of 1st DP principle:

- Personal data must be processed fairly, lawfully and in a transparent manner (Art. 5(1)(a); Recital 39)

- Controller is responsible for demonstrating compliance with transparency (Art. 5(2))

- Controller must provide information and all communications to individuals in a concise, transparent, intelligible and easily accessible form, using clear and plain language (Art. 12(1)), in respect of:

    - Privacy notices when data is collected from data subject (Art. 13) or third parties (Art. 14)

    - Individual rights: right of access (Art. 15), right of rectification (Art. 16), right to erasure (Art. 17), right to restriction (Art. 18), notification re rectification, erasure or restriction (Art. 19), data portability (Art. 20), right to object (Art. 21), automated decision making, including profiling (Art. 22)

    - Notifications of personal data breach (Art. 34)

See also Recitals 39, 58, 60-63 - individuals must be made aware of processing, purposes, risks, rules, safeguards and rights

Transparency is further reinforced by and linked to GDPR requirements for consent, notice, legitimate interest, right of access, publicising DPO contacts.

- **Privacy Notice (Art. 13 & 14)**

  Controllers must provide the following information to individuals **when obtaining data from individuals** and **when obtaining data from third parties**:

    - Controller/representative identity

    - DPO identity/contact details

    - Purposes of processing and legal basis

    - If processing based on legitimate interests, an explanation of those interests

    - Whether provision of data is mandatory

    - Recipients

    - Data retention periods

    - All individuals' rights, including right to complain to DPA

    - Information on cross-border transfers

- Existence of automated decision taking and logic behind it
- Not necessary where individuals already have this information
- Further exemptions from notice when collecting data from third parties – impossible or disproportionate effort, legal obligation, confidentiality duty (Art. 14(5))
- Standardised machine readable policies and icons are encouraged and Commission can set the information provided by icons and procedure for standardised icons (Art. 12(7)(8))

GDPR Consent Requirements

- Consent is one of the grounds for lawful processing (Art. 6(1)(a)), key ground for processing of sensitive data (Art. 9), one of the basis for data transfers outside EU (Art. 49)
- Consent must be freely given, specific, informed and unambiguous indication by statement or clear affirmative action (Art. 4(11); Recital 32)
- Controller must be able to **demonstrate** consent, if a basis for processing (Art. 7(1); Recital 42)
- Request for consent must be intelligible and easily accessible using clear and plain language (Art. 7(2); Recital 42)
- DP Consent must be **distinguishable** from other consents and **separate for each processing operation** (Art. 7(2))
- Consent can't be used where there is **clear imbalance** between individuals and controller (Recital 43), in particular where controller is a public authority
- Consent must **not be conditional** – contract/ service must not be conditional on consent to processing not necessary for the contract/service (Art. 7(4); Recital 43)
- Individuals can **withdraw** consent any time (Art. 7(4); Recital 42)
- **Children's consent**: can be used if child is at least 16. If below 16, consent must be "given or authorized" by the parent (Article 8(1)) (Member States may lower the age 16 -13. Art. 8(1))

GDPR Legitimate Interest Requirements

- One of grounds for **lawful processing** of personal data (Art. 6(1)), as well as an exceptional basis for data **transfers outside the EU** (Art. 49(g))
- Processing is necessary for the purpose of the legitimate interests by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedom of the data subject, in particular where data subject is a child (Art. 6(1)(a), (f); Recitals 47, 51)
    - Controller must take into consideration individual's **reasonable expectations based on his/her relationship with controller** (Recital 47)
    - Controller must provide **notice** of legitimate interest to individuals.

- Examples of recognised legitimate interest in GDPR (Recitals 47-49):
    - Fraud prevention
    - Information and network security
    - Direct marketing
    - Processing by a group of undertaking for internal administrative purposes, including clients' and employees' data (but without prejudice to cross border data transfers requirements)
- Individuals have a broad **right to object** to processing based on legitimate interests, at any time and without justification, but the controller may demonstrate compelling interests overriding the right of the data subject (Art. 21)
- Legitimate interest processing not available for processing of special categories of personal data (Art. 9), or for automated decision making that produce legal effects or significantly impact individuals, or for data processing in the context of ePrivacy Regulation (*lex specialis* applies)
- Legitimate interest may be used exceptionally for data transfers outside the EU on a limited basis (Art. 49(g)(2)) - no other ground and derogation applies, not repetitive transfers, limited number of individuals' interests must be "compelling" and controller must assess all the circumstances and provide suitable safeguards
    - Controller must inform DPA and individual of the transfer and the use of the compelling legitimate interest

APPENDIX II:
CIPL Examples of Legitimate Interest Grounds for Processing of Personal Data

In preparation for CIPL GDPR Project Madrid Workshop III, CIPL has asked the GDPR project members for examples where a) legitimate interest is the appropriate ground for processing personal data, and b) in some cases the only legal ground for processing.

The purpose of the exercise was to establish current practices and instances of organisations using legitimate interest processing under the current law and to inform all the stakeholders involved in the GDPR implementation of the broad application of this ground of processing today.

Part I of this document is a summary of the examples we received, organised in broad categories of processing purposes. Part II are specific case studies from different industry sectors that provide an in-depth discussion of the rationale for legitimate interest processing, and the balancing of interests and risk mitigation undertaken by the controller to ensure accountability and to meet the reasonable expectations of the individual.

The examples we received demonstrate the following:

a) organisations in all sectors currently use legitimate interest processing for a very large variety of processing personal data and this trend is likely to continue under the GDPR.
b) in many cases, legitimate interest processing is the most appropriate ground for processing, as it entails organisational accountability and enables responsible uses of personal data, while effectively protecting data privacy rights of individuals.
c) in some cases, organisations use legitimate interest as the only applicable ground for processing, as none of the other grounds can be relied on in a particular case.
d) organisations using legitimate interest always consider the interest in case (of controller or a third party / parties); they balance the interest with the rights of individuals; and they also apply safeguards and compliance steps to ensure that individuals rights are not prejudiced in any given case.
e) the current use cases of legitimate interest tend to form a pattern, with most common examples being prevalent in many organisations and all the cases broadly falling in several wide categories outlined below. The most prevalent category of legitimate interest cases across all industries is i) fraud detection and prevention and ii) information and system security.

PART I:

Summary of categories and examples of legitimate interest processing

1. Fraud detection and prevention (crime prevention)

Many companies need to process certain personal data to comply with industry standards, regulators' requirements and other requirements related to fraud prevention and anti-money laundering. These are often financial institutions such as banks, credit card issues and insurance companies, but also other organisation in consumer-facing businesses and they often need to process data in a global context. Specific examples are:

- Fraud and financial crime detection and prevention
- Anti-money laundry (AML) Watch-lists
- Know-your-customer (KYC)
- Credit checks and risk assessments
- Politically Exposed Persons (PEP)
- Terrorist financing detection and prevention
- Anti-fraud purposes - using information gathered from various sources, such as public directories and publicly available online personal or professional profiles, to check identities when purchases are deemed as potentially fraudulent
- Defending claims, e.g. sharing CCTV images for insurance purposes

2. Compliance with foreign law, law enforcement, court and regulatory bodies' requirements

Organisations in all sectors are subject to a multitude of laws and regulations; to reporting obligations to regulators; to regulators', law enforcement and judicial requests and regulations, including from specific industry regulatory bodies, such as health or financial regulators, both within EU and abroad. Global companies are often subject to many competing laws, which sometimes appear to be in direct conflict with data privacy laws elsewhere. Organisations are often compelled to use legitimate interest processing in some of these instances to base processing and sharing of some personal data where they are sufficiently able put in place mitigations and safeguards for rights of individuals. Specific examples are:

- Operation of Business Conduct and Ethics Line and Reporting under the Sarbanes-Oxley Act (SOX)
- Economic sanctions and export control list screening under economic sanctions and export control laws
- Data loss prevention software and tools for compliance with data protection laws and client contractual requirements
- Compliance with requests for disclosures to law enforcement, courts and regulatory bodies, both EU and foreign

3. Industry watch-lists and industry self-regulatory schemes

Organisations in credit industry, banking, finance, insurance, retail often need to process certain personal data to protect and develop industry standards; share intelligence about individuals or concerns that may have a negative or detrimental impact; to set pricing; and to follow industry best

practices. Specific examples are:

- Industry watch-lists – non-payment, barred customers, etc.
- Relations with insurers – information to process insurance claims
- To comply with industry practices (issued by the Financial Action Task Force (FATF), Wolfsberg AML Principles, etc.)

4. Information, system, network and cyber security

All organisations need to monitor, detect and protect the organisation, its systems, network, infrastructure, computers, information, intellectual property and other rights from unwanted security intrusion, unauthorised access, disclosure and acquisition of information, data and system breaches, hacking, industrial espionage and cyberattacks. Organisations will inevitably process personal data as part of the purposes stated above, including of direct clients and customers, third parties, employees and any other people who may have access to company systems and networks. Legitimate interest processing is often the only ground that organisations can rely on for this type of processing.

These type processing are conducted by all organisations, in both public and private sector and all lines of industry. Specific examples are:

- Overall information security operations of an organisation to prevent unauthorised access, intrusion, misuse of company systems, networks, computers and information, including prevention of personal data breaches and cyber attacks
- Piracy and malware prevention
- IP rights protection and IP theft prevention
- Website security
- Monitoring access to systems and any downloads
- Use of information gathered form physical access control systems for investigating incidents
- Detection and investigation of security incidents – processing of personal data of individuals involved in an incident, as well as the underlying compromised data
- Investigation and reporting of data breaches
- Product and product user security

5. Employment data processing

Irrespective of industry, organisations process employees' data for legitimate and common business purposes, in situations which are not necessary for the performance of employment contract, but are nevertheless customary, or necessary for operational, administrative, HR and recruitment purposes and to otherwise manage employment relationship and interaction between employees. Specific examples are:

- Background checks and security vetting in recruitment and HR functions
- Office access and operations
- Disaster and emergency management tools and apps
- Internal directories, employee share-point sites, internal websites and other business cooperation and sharing tools.
- Business conduct and ethics reporting lines

- Compliance with internal policies, accountability and governance requirements and corporate investigations
- Call recording and monitoring for call centre employees' training and development purposes
- Employee retention programs
- Workforce and headcount management, forecasts and planning
- Professional learning and development administration
- Travel administration
- Time recording and reporting
- Processing of family members' data in the context of HR records – next of kin, emergency contact, benefits and insurance, etc.
- Additional and specific background checks required by particular clients in respect of processors' employees having access to clients' systems and premises
- Defending claims - sharing CCTV images from premises with insurers when required for processing, investigating or defending claims due to incidents that have occurred on our premises
- Intra-corporations hiring for internal operations

6. General Corporate Operations and Due Diligence

All organisations, irrespective of the sector, use personal data to operate the day-to-day running of the business and plan for strategic growth. This includes management of customer, client, vendor and other relationships, sharing intelligence with internal stakeholders, implementing safety procedures, and planning and allocate resources and budget. Specific examples are:

- Modelling – develop or operate financial/credit/conduct and risk models
- Internal analysis of customers – plan strategy and growth
- Reporting and management information – support business reporting
- Sharing information with other members of the corporate group
- Back-office operations
- Monitoring physical access to offices, visitors and CCTV operations in reception and any other restricted areas
- Processing of personal data of individuals at target company or related to the transaction in M&A transactions
- Corporate reorganisations
- Producing aggregate analytics reported to third party content owners, especially when it is to fulfil licensing obligations
- Business intelligence
- Managing third party relationships (vendors, suppliers, media, business partners)
- Processing identifiable data for the sole purpose of anonymising/de-identifying/re-identifying it for the purposes of using the anonymised data for other purposes (product improvement, analytics, etc.)

7. Product development and enhancement

All organisations process personal data to deliver and improve their products or services. Many technology companies need to process data collected from their services or products in order to deliver that service, or to instruct their products how to work and to continuously keep on improving

them. Specific examples are:

- Processing of personal data for research, product development and improvements – such as integrity and fairness of a process/service; or data collected by voice recognition tools, or translation tools, which all depend on ability to collect a lot of data of direct customer and other individuals to be able to create and improve the actual service
- Processing of most device data (including the hardware model, operating system version, advertising identifier, unique application identifiers, unique device identifiers, browser type, language, wireless network, and mobile network information) to improve performance of the app, troubleshoot bugs, and for other internal product needs.
- Information from GPS on smartphones where the chip in the phone needs to provide location data in order to pick up satellite information
- Collection of IP addresses and similar by telecommunication companies that may need to use several unique identifiers to enable them to provide connectivity as well as charge the appropriate person.
- Log files/actions within apps for product use analysis, product performance enhancement and product development
- Monitor use and conduct analytics on a website or app use, pages and links clicked, patterns of navigation, time at a page, devices used, where users are coming from etc.
- Monitor queues at call centres

8. Communications, marketing and intelligence

Organisations across all the sectors process certain personal data to gather market intelligence, promote products and services, communicate with and tailor offer to individual customers. In addition to B2C, many organisations also use legitimate interests in the context of marketing and communications with B2B customers and contacts. Specific examples are:

- Discretionary service interactions - customers are identified in order for them to receive communications relating to how they use and operate the data controllers' product
- Personalised service and communications
- Direct marketing – of the same, or similar, or related products and services; including also sharing and marketing within a unified corporate group and brand;
- Targeted advertising
- Analytics and profiling for business intelligence – to create aggregate trend reports; find out how customers arrive at a website; how they use apps; the responses to a marketing campaign; what are the most effective marketing channels and messages; etc.
- Ad performance and conversion tracking after a click
- Audience measurement – measuring audiovisual audiences for specific markets
- Mapping of publicly available information of professional nature to develop database of qualified professionals/experts in relevant field for the purpose of joining advisory boards, speaking engagement and otherwise engaging with the company
- B2B marketing, event planning and interaction

PART II: Specific case studies

The following case studies have been contributed by CIPL GDPR Project members and selected to illustrate the breadth and scope of legitimate interest as the legal processing ground across industry sectors. The cases follow a similar pattern, but with some variance in format to highlight the various issues and topics that each individual example addresses.

1. Case: Creation and/or Use of Watch Lists to Meet Anti-Money Laundering (AML), Politically Exposed Persons (PEP), Anti-Fraud or Diligence Obligations

Rationale for legitimate interest processing: To protect the international financial system from abuse, financial institutions and other companies must often screen new and existing customers or vendors against watch lists. The lists are designed to help financial institutions determine if a business relationship might carry a risk of financial or other crime. The source of this obligation must be either Member State law, laws of non-EU countries; or even just good business practices designed to reduce regulatory or financial risk.

The source of the information that goes on the watch list may for example be private entities using publicly available information of Politically Exposed Persons (PEPS) or sanctions published by national or international organisations. Given the nature of such lists, it is not feasible for the creator to obtain consent from the individual regarding the inclusion of their personal data, so the creator must use legitimate interest as their processing ground. Note the Fourth AML Directive explicitly authorises financial institutions to use third party service providers to provide watch lists, as it may be the only way an institution can meet its AMLs obligations. Equally, for some instances, controllers that perform checks against the officially published watch lists and conduct the screening activities themselves also must rely on legitimate interest in order to process personal data of people on the lists.

GDPR legitimate interest balancing: The data processing should be relevant, adequate and limited to what is necessary for its purpose. The public and private interests served by such diligence meet the legitimate interest requirements as long as the interests or the fundamental rights and freedoms of the individual are not overriding. Those public or private interests may include fraud prevention, stability of the financial system, preventing market abuse, investor protection, combatting money laundering and combatting terrorism.

Mitigation and reasonable expectation: Satisfying the legitimate interest basis for processing also requires accurate and fair procedures in the creation and use of the lists. It is imperative that the processing parties have applied the necessary safeguards under the GDPR for the processing of this data. For example, the vendor of a list must have a DPO and the individual must have the opportunity to correct inaccurate information. However, the right to correct inaccurate information is not absolute, as EU and Member State law can impose limitations in the context of public good or national security or defence interests in the public good. For example, this may also cover the obligations of public or private entities as publishing a list of potentially fraudulent IP addresses might inform criminals by omission of IP addresses that may still be used for fraud.

2. Case: Fraud monitoring, detection and prevention

Rationale for legitimate interest processing: Financial institutions, payment networks and other companies must process personal data of individuals in order to monitor, detect and prevent fraud. In particular, payment networks are in a unique position to monitor and detect signs of fraud across all participants in the payment eco-system. They can alert financial institutions that a payment

transaction is likely to be fraudulent in real-time, so that the financial institutions can notify the affected individual cardholders and/or make a decision as to whether to approve or deny a payment transaction.

The EU Payment Services Directive 2007/64/EC sets out that "*Member States shall permit the processing of personal data by payment systems and payment service providers when this is necessary to safeguard the prevention, investigation and detection of payment fraud*"". However, the majority of anti-fraud activities are performed under regulatory and sectorial obligations, rather than EU or Member State law. Payment networks and financial institutions are indeed subject to the oversight of the European Central Bank and relevant National Banks and, as such, must comply with recommendations and standards to ensure an adequate degree of security, operational reliability and business continuity. This includes the implementation of robust measures to combat fraud. Moreover, EU and national governments and policymakers increasingly expect all parties in the payment eco-system to be more active in this space. The effective fight against fraud is indeed key to boost individuals' trust in the digital economy.

GDPR legitimate interest balancing: The legitimate interest of the payment network to protect its network and its brand meets the interests of all parties in the payment ecosystem, namely financial institutions and merchants to minimise the fraud impact and losses, as well as individual cardholders to be protected against fraud. Individual cardholders actually expect their payment transactions to be processed in a safe and secure way.
The outcome of the balance of interests test is properly documented and, where appropriate, a full Data Protection Impact Assessment is conducted to ensure adequate and effective data protection.

Mitigation and risk assessment: Prior to launching a new anti-fraud tool, the payment network assesses whether there are less invasive means to achieve the same purpose. To further mitigate the potential risks and enhance the protection of the individuals' interests and fundamental rights and freedoms, additional safeguards and controls are implemented by the payment network as needed, such as strict data access, data use limitations, security measures, retention schedules, as well as data minimisation including as appropriate data anonymisation and pseudonymisation.

Limits of consent: Obtaining consent from individuals for collecting and using their data for anti-fraud purposes would not be workable or meaningful. Indeed, all good faith individuals would agree to provide their consent while fraudsters would withhold their consent. This would result in missing information making fraudulent activity increasingly difficult to monitor and/or to detect. Ultimately, this would jeopardise the financial stability, reliability and integrity of the payment network, thereby harming all legitimate parties in the payment ecosystem including individuals themselves.

3. Case: Processing of data in relation to M&A

Rationale for legitimate interest processing: In the context of an M&A transaction, there may be a need to make available and review documentation containing personal data, and to prepare transaction documents based on these. The documentation may contain personal data (i) incidentally, such as names and other details of those executing agreements and notarial deeds, the proxyholders, the identity of the members of the corporate management bodies, the identity of individuals involved in litigation actions initiated by or against the relevant company, etc. or (ii) purposefully, such as the employment documentation that must be reviewed, particularly to determine the appropriate conditions of the transfer of the workforce and, if transferred, whether the documentation appropriately evidences the compliance with the applicable requirements that the "buyer" may inherit (e.g. social security payments).

M&A transactions (with third parties or intra-group) may be structured, as a general rule, either through share deals or asset deals. Asset details may entail a universal succession of rights and liabilities (e.g. a merger or a split off) or transfers "uti singuli" (e.g. a sale and purchase agreement. Some may entail a transfer or undertaking from an employment law point of view, and some may entail the transfer of a business unit from a tax law point of view. What is common in all of these transactions, for the purposes of legitimate interest, is that the potential acquirer is interested in pursuing the same activity as the seller (if not, other legal grounds would not need to be assessed).

In all of these transactions, the review of the documentation that may contain personal data must be undertaken by the potential acquirer (e.g. the buyer or the beneficiary of the company, the asserts or the business unit) and seller, as well as its external advisors (lawyers, IT consultants, financial auditors) in order to determine the initial and final scope of the subject-matter of the acquisition (which would need to be described in the transaction documents, the potential legal, financial and operational contingencies, the condition precedents for closing and the price of the transaction). Hence, all of these parties processing personal data would rely on the legitimate interest ground to be able to proceed with their tasks.

GDPR legitimate interest balancing: There is a clear legitimate interest in carrying out such review with appropriate safeguards in place to protect that there is no deviation of the legitimate purpose due to the NDA agreements. These may include information being made available to individuals with access rights on a need-to-know basis. To anonymise the data is not only a huge effort for the selling company (in terms of cost and time but will prevent the transaction from being properly designed (e.g. you need to identify the owners of the shares or the assets; who is an authorised signatory, etc. or jeopardise the review since many contingencies can only be detected if identifiers exist (e.g. labour contingencies, litigation, non-compete provisions regarding senior executives).

Mitigation and risk assessment: Before any M&A review, a non-disclosure agreement is always executed among all the involved parties in order to protect the exchange of information, which is by nature, commercially sensitive (irrespective of whether personal data are contained or not). The review could be made by marking available documentation in platforms held by third parties in "view only" as well as a general rule (upon request, the reviewers may ask to have copies of specific documents with no personal information).

Limits of consent: Informed consent is not an option. This is not only because it would involve disproportionate effort, but because confidentiality should be preserved until the transaction is closed (vis-à-vis employees, the clients or the capital markets). The closing of a M&A transaction cannot depend on the consent, or its withdrawal for data protection reasons (if specific groups must be protected, other laws would provide such protection, such as minority shareholders protected by corporate laws; employees protected by employment laws etc.

4. Case: Internet Protocol Addresses

Rationale for legitimate interest processing: Much like a house or apartment in the physical world, computers that are connected to the Internet are assigned an address called an "Internet Protocol Address" or "IP Address" for short. Those addresses can be "dynamic" which means they change each time the computer connects to the Internet, or they can be "static" which means that they are fixed. When a computer requests a web page or other content on the Internet, it sends its IP address to the computer hosting that content asking the server to return the content to its IP address. Without the address, the server would not know where to send the content. For most companies, that IP address is simply either (a) the computer requesting the content, or (b) the identity of the computer hosting the content. In addition to using the IP address for sending or receiving content,

however, companies can also use the IP address for internal business purposes such as security (for example to detect and prevent "denial of service" attacks where an attacker can overload a server by sending superfluous requests for a web page), or to measure website traffic. The exception, however, is the Internet Service Provider (or ISP) who is providing the connectivity. ISP's often have information linking the IP address to the individual subscriber in order to provide technical support, billing, and other business purposes related to their service.

GDPR legitimate interest balancing: The data processing should be relevant, adequate and limited to what is necessary for its purpose. The public and private interests served by such use of the IP address meet the legitimate interest requirements as long as the interests or the fundamental rights and freedoms of the individual are not overriding. In this case, delivery of content on the internet would simply not be possible without the IP address just like sending or receiving physical mail in the real world. And internet content owners certainly have a legitimate interest in protecting their content and services from bad actors. Apart from the legitimate interest ground, none of the other Art. 6 processing grounds allowing for the lawfulness of processing of the IP address would be applicable in this case.

5. Case: Providing Location Through Terrestrial Wireless Signals

Rationale for legitimate interest processing: Location based services, or LBS, provide significant value to individuals and are a key feature of multiple products and services used today. But LBS loses its usefulness if wireless devices cannot readily determine location in urban environments or deep indoors. In such environments, using satellite positioning technology alone, such as GPS or Galileo, is slow and uses substantial power. One way to speed up location determination and save battery life is to determine location by detecting nearby wireless access points such as Wi-Fi routers and cell towers and comparing those access points to data stored on the device. Such data stored on the device is essentially a look-up table containing Wi-Fi routers' and cell towers' unique IDs and associated locations. Using Wi-Fi signals is particularly important because it enables indoor LBS services where accessing navigation satellites is limited or impossible.

Limitations of consent: Maintaining an up-to-date list of locations of Wi-Fi routers is a continuous process because Wi-Fi routers are frequently added or removed from the internet. Thus, companies frequently collect this information through a variety of sources, including from individual smartphones as they move about the environment. Getting consent from the smartphone owner is certainly possible for the service provider, operating system provider, or device provider because of the direct relationship between the smartphone owner and these companies. . These companies, however, often do not have a direct relationship with the owner of the Wi-Fi access point, thereby making obtaining their consent impracticable and unfeasible. According to the WP29, the owner of the Wi-Fi router has a privacy interest in their router's unique ID in combination with its location. But because of the lack of a relationship with router's owner, the only lawfulness mechanism applicable to collect such information is legitimate interest.

6. Case: Processing for Targeted Advertising and Service Personalisation (Recital 47)

Rationale for legitimate interest processing: Direct marketing may be a legitimate interest in accordance with GDPR Recital 47. Equally, the WP29 has stated in its guidance on legitimate interests that: "controllers may have a legitimate interest in getting to know their customers' preferences so as to enable them to better personalise their offers and ultimately, offer products and services that better meet the needs and desires of the customers."

The same rationale should apply to other forms of targeted marketing, including advertising based on a person's online activity. Targeted advertising should be deemed to fall within the controllers and third parties' legitimate interests and not be outweighed by the individual's rights, provided the data are used in accordance with the specific requirements, the individual receiving the advertising is given information about how their data will be used for targeting and has meaningful controls over those uses. The controller must also be accountable for honouring the choices individuals have made regarding how their data are used for ads.

Advertising is one of the primary business models of free services, a fact all users of free services are well aware of. Personalisation of content and offering is a core feature of many services – it makes the service what it is. Without personalisation, many services would lose business as their customers and users rely on personalisation as one of the value propositions of the service. Therefore, controllers should be able to rely on legitimate interest as the basis for processing of the personal data of their users for personalisation of content and offerings.

GDPR legitimate interest balancing: In considering targeted advertising through the lens of the legitimate interests balancing test, this test should take into account interests of multiple actors. The growing evidence shows both the importance of targeted ads to the business models of many online publishers and advertisers and the fact that relevant ads can create real value for individuals by helping them discover new products, services, and causes, and by helping to avoid subjecting individuals to discriminatory advertising. Businesses clearly have legitimate interests in providing targeted advertising for these purposes.

Mitigation of risk: For similar reasons, personalisation has become the hallmark of many of the world's most popular online services, which has led individuals not only to expect, but to demand that websites and apps use their personal data to personalise their experience. The value personalisation creates for people and for businesses (which benefit from increased engagement) is clear. To mitigate privacy risks, organisations put in place measures to ensure that service personalisation usually does not involve sharing personal data with third parties, or making decisions about the individual that could have an adverse effect and create harms to individuals.

The widespread availability of controls around targeting advertising (such as controls offered by the European Interactive Digital Advertising Alliance) have helped address individuals' privacy interests, as have the enhanced commitment of commercial players to educate consumers regarding how advertising works on their services and how individuals can make relevant choices about their advertising experiences. Moreover, some companies have gone ever further in giving users more transparency and more granular controls over how their data is used to show them relevant ads. Coupled with internal safeguards and compliance measures employed by organisations, these efforts should mitigate any privacy risks to the individuals that receive targeted ads.

Reasonable expectations of the individual: Individuals have come to expect and understand that they will receive targeted advertising based on their personal data and preferences, particularly when using free online services. These expectations are clearest where the consumer has a direct relationship with the company that provides the advertising. Third-party providers can also enable this understanding by providing improved transparency themselves, or through the first parties with which they work.

Limits of consent: Legitimate interests in some cases may be a more appropriate legal basis than consent because of the way the online advertising ecosystem works. In many, if not most, targeted advertising scenarios, multiple parties will be involved in serving the targeted advertisement. It often will be infeasible for each of these parties to obtain individuals' consent (and provide the

mechanism for withdrawal) that the GDPR requires. More importantly, however, requiring each of these parties to obtain consent would result in the individuals being overwhelmed by consent requests and burdened by having to manage them all. Research has shown that in these scenarios, individuals are less likely to pay attention to notices and consents and more likely to simply click through, in order to receive a service or access information that they want. This leaves people in a position where they are actually less empowered.

7. Case: Audience Measurement ("AM")

Rationale for legitimate interest processing: Audience Measurement ("AM") is a way to measure audiences for specific markets (e.g. TV, radio, newspapers, or websites). It is distinct from advertising and cannot be used to target individuals for advertising. Different AMs (e.g. surveys, panels and online measurements) have distinct methodologies and rely on different legal grounds. For example, TV measurement panels involve a large number of households and currently requires the installation of a special box that measures viewing behaviour, based on a contractual relationship. Surveys are carried out by fieldworkers and rely on consent, while online measurements require the content owner to include tag that allows the AM provider to place a cookie.

AM provides information regarding market size, business analytics and allows for the independent verification of viewing for billing purposes. AM also serves to ensure that copyright royalties are calculated precisely. The outcome of AM are reports that show aggregate data: they do not permit the identification of any individuals, but are usually grouped under relevant geodemographic headings (e.g. age-brackets, gender, geographical distribution, socio-economic parameters).

GDPR legitimate interest balancing: When conducting the balancing test under the legitimate interest ground one has to consider multiple rights and interests - the privacy right of the individual, the rights of media owners, the right to conduct a business, and AM providers' interests. In balancing how the right to conduct business and the AM provider's interest are pursued with the rights of individuals, the intrusion into privacy is minimal: WP29 has recognised that web analytics pose minimal privacy risks. This ought to be even more the case where the AM provider cannot link the data to an account or a registered user, which a website can do with web analytics. The objective of AM is to produce aggregate reports that consists of anonymous data. At an individual level, data are psedonymised and not retained beyond the original purpose.

AM helps market function more efficiently and competitive and also help fund free and quality media. A lack of effective AM would lead to opaque markets and leave advertisers in the dark, which would impact media funding negatively.

Mitigation and risk assessment: risk to the individual are limited by deploying privacy safeguards, including:

- Strict purpose limitation – no AM data is used to direct advertising to individuals
- Providing opt-outs
- Truncating IP addresses and subsequent one-way hashing/pseudonymisation
- Anonymisation - clients only receive aggregate reports
- Contractual safeguards with suppliers and partners and prohibition to re-identify data

AM providers draw a line between third party independent measurements and advertising. AM reports are not intended or suitable for advertising or to target individuals for marketing purposes. Instead, AM can provide verification that content has reached its intended demographic segment,

whether that is for content or for advertising purposes. Any intrusion on privacy is minimal and individuals always have the opportunity to object to the processing or delete their cookies. AM cookies are not used to re-identify individuals or allow those users to be targeted for advertising or other marketing purposes.
Limits of consent: The legitimate interest ground is the cornerstone for enabling the benefits of AM activity in the ecosystem, both for media owners as much as for AM providers. Legitimate interest is the only practical available ground for processing because the data collected typically does not enable identification of the individual. Also, consent would generally be performed in such a way as to make obtaining user consent unduly burdensome. Indeed, the accuracy of the measurement in the digital and mobile areas would likely be greatly diminished if consent was required, due to typically low participation rates where opt-in is required.

AM companies, just like processors and IT service providers, are unknown to users and do not have a direct relationship with the individuals or provide a direct consumer benefit. Media companies are also very reluctant to request providers to collect consent individually, as this would pose a major disruption and favour companies that have those capacities in-house or have already obtained consent via different means (which would undermine the unbiased and neutral features of AM activities).

12 April 2017

Discussion Paper

Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms

Centre for Information Policy Leadership GDPR Implementation Project
April 2017

CIPL's TOP TEN MESSAGES ON GDPR CERTIFICATIONS

1. Certification should be available for a product, system, service, particular process or an entire privacy program.

2. There is a preference for a common EU GDPR baseline certification for all contexts and sectors, which can be differentiated in its application by different certification bodies during the certification process.

3. The Commission and/or the EDPB, in collaboration with certification bodies and industry, should develop the minimum elements of this common EU GDPR baseline certification, which may be used directly, or to which specific other sectoral or national GDPR certifications should be mapped.

4. The differentiated application of this common EU certification to specific sectors may be informed by sector-specific codes of conduct.

5. Overlap and proliferation of certifications should be avoided so as to not create consumer/stakeholder confusion or make it less attractive for organisations seeking certification.

6. Certifications must be adaptable to different contexts, scalable to the size of company and nature of the processing, and affordable.

7. GDPR certifications must be consistent with and take into account other certification schemes with which they need to be able to interact and/or be as much interoperable as possible, such as ISO/IEC Standards, EU-US Privacy Shield, APEC CBPR and the Japan Privacy Mark.

8. Developing a common EU-wide GDPR certification for purposes of data transfers pursuant to Article 46(2)(f) should be a priority for the Commission and/or the EDPB.

9. Organisations should be able to leverage their BCR approvals to receive or streamline certification under an EU GDPR certification.

10. DPAs should incentivise and publicly affirm certifications as a recognised means to demonstrate GDPR compliance, and a mitigation in case of enforcement, subject to the possibility of review of specific instances of non-compliance.

1. INTRODUCTION

1.1 Certifications, seals and marks under the GDPR as promising instruments for data protection

Certifications, seals and marks have the potential to play a significant role in enabling companies to achieve and demonstrate organisational accountability and, more specifically, GDPR compliance for some or all of their services, products or activities. The capability of certifications to provide a comprehensive GDPR compliance structure will be particularly useful for SMEs. For large and multinational companies, certifications may, in addition, facilitate business arrangements with business partners and service providers.

However, certifications must not be made mandatory, but should be treated only as one of many optional tools for companies. There must be no inference of non-compliance if a company chooses not to obtain certification.

In addition, certifications, seals and marks can be used as accountable, safe and efficient cross-border data transfer mechanisms under the GDPR, provided they are coupled with binding and enforceable commitments, including with regard to data subject rights. Finally, there is potential for creating interoperability with other legal regimes, as well as with similar certifications, seals and marks in other regions or in other policy domains.

These instruments present real benefits for all stakeholders, including DPAs and, most importantly, individuals. They have the potential to assist organisations in delivering better compliance and more effective protection for individuals given that certified organisations will have made a conscious effort to become GDPR compliant and will have been reviewed by a third party in that respect.

This is why CIPL generally supports the certifications, seals and marks in the GDPR. However, it is crucial that certifications are effectively operated, incentivised and clearly accompanied by benefits for certified organisations. Otherwise, organisations will be reluctant to invest time and money in obtaining and maintaining GDPR certifications on top of the many other certifications and requirements to which they are already subject.

1.2 The CIPL GDPR Project

This paper is produced by the Centre for Information Policy Leadership at Hunton & Williams (CIPL) as part of its project (CIPL GDPR Project) on the consistent interpretation and implementation of the GDPR.

The CIPL GDPR Project—a multiyear-long project launched in March 2016—aims to establish a forum for dialogue amongst industry representatives, the EU DPAs, the European Data Protection Supervisor, the European Commission, the ministries of the member states and academics on the consistent interpretation and implementation of the GDPR through a series of workshops, webinars, white papers and comments.

CIPL aims to provide input to the Article 29 Working Party (WP29) on a number of priority areas, identified in CIPL's GDPR Project work plans for 2016 and 2017.[1] This is the fourth white paper in this series, following earlier CIPL papers on DPO, Risk, and OSS and Lead Authority.[2]

1.3 CIPL's Certifications Paper

In this paper, CIPL aims to provide the WP29, the EU Commission and data privacy practitioners with input on certifications, seals and marks under the GDPR and the roles of these instruments as accountability tools and cross-border data transfer mechanisms.

The paper intends to facilitate the development of certifications, seals and marks under the GDPR[3] in a way that is pragmatic and benefits all stakeholders.[4]

CIPL notes that there are both similarities and differences between certifications and approved codes of conduct under the GDPR. Although the synergies between both tools must be identified, CIPL will address codes of conduct separately, at a later stage.

2. BENEFITS OF CERTIFICATIONS

Adherence to approved certification mechanisms under Article 42 GDPR may be used as an element in demonstrating compliance with the GDPR obligations of the controller and processor. Moreover, certification mechanisms have the potential to significantly contribute to effective and efficient privacy protection for individuals in a globalised world. They should evolve into real bridges between different legal regimes and accountability frameworks.

Specifically, CIPL has identified the following benefits of certifications to key stakeholders—individuals, organisations, DPAs and the overall digital ecosystem:

2.1 Benefits for individuals

Certifications carry tangible benefits for individuals.

- **Create trust.** Certifications have the potential of increasing individuals' trust and confidence in a certified organisation's handling of their personal data. This in turn may result in individuals'

[1] See https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_work_plan_17_march_2017.pdf

[2] See https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_gdpr_dpo_paper_17_november_2016.pdf; https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_the_gdpr_one-stop-shop_30_november_2016.pdf; https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf

[3] See Appendixes I and II for a summary of the GDPR certification provisions.

[4] In this paper, we will use the term "certifications" to encompass seals and marks (without foreclosing a discussion about whether there can be differences between these three concepts).

wanting to engage more with a certified organisation and participating in the digital economy more freely.

- **Greater transparency.** Certification ensures better transparency of processing practices of the organisation, making it easier for individuals to understand and assess relevant data practices and their merits.

- **Effective privacy protection.** Individuals may regard certification as a demonstration of commitment to and compliance with effective and rigorous data protection and complaint resolution practices. Adherence to certification mechanisms by organisations ultimately may deliver better compliance and outcomes for individuals, with their data's being more effectively protected.

2.2 Benefits for Certified Organisations

If implemented effectively, certifications may convey a number of key benefits to organisations.

- **Demonstrate accountability and compliance.** Certification is an element of demonstrating GDPR compliance and accountability.[5] This is an internal benefit vis-à-vis management, the board and shareholders. It also benefits an organisation externally in its relationships with DPAs, individuals, clients and business partners. It builds confidence and trust in the organisation with these external stakeholders, as well as with the wider public.

- **Operationalising compliance.** Certifications translate high-level GDPR requirements into operational compliance steps that are closely tailored by subject-matter experts to the organisation and their privacy management programs. This may result in more relevant, fit-for-purpose and effective privacy and data management programs.

- **Scalable for SMEs and start-ups.** For SMEs and start-ups, well-conceived and properly implemented certifications can serve as scalable and at the same time comprehensive compliance mechanisms that make relevant GDPR accountability obligations less burdensome, less costly and easier to implement, in particular for organisations that do not yet have fully developed privacy management programs or their own internal privacy experts and staff. The third-party certification body will have the expertise and the obligation to ensure that the certifying organisation has policies and processes in place that comply with the GDPR. This improves both organisational compliance and privacy protections for individuals.

- **B2B due diligence and risk management.** In B2B relationships, certification may efficiently demonstrate GDPR compliance and accountability on the part of the processor or service provider. For the same reason, it may also serve as an effective risk-management tool in B2B relationships by lowering the risk profile of the certified processors or providers, thereby directly lowering the risk level of the involved processing as well as the need for DPIAs and/or prior consultations with DPAs.

[5] Article 24(3) GDPR.

- **Enabling cross-border data transfers.** Certification provides legal certainty to organisations by enabling them to share personal data lawfully outside the EU and across borders, provided that certification is coupled with binding and enforceable commitments.

- **Interoperable and global reach.** 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, thereby extending the certification's geographic coverage and reach. Examples of systems with which GDPR certification could be made interoperable include the ISO Cloud Privacy and Security Standard, the Japan Privacy Mark and the APEC Cross-Border Privacy Rules (CBPR).

- **Mitigating factor in DPA oversight and enforcement**. In addition to serving as demonstration of compliance in the context of audits or other inquiries by DPAs, certification is potentially a mitigating factor in connection with GDPR enforcement and the determination of sanctions.

2.3 Benefits for DPAs

Certification mechanisms have the potential for supporting the oversight missions of DPAs and making it possible for them to leverage their scarce resources more effectively.

- **Reduce oversight workload.** Where certification bodies take on and share the burdens of supervision and oversight with the DPAs, this has the potential of reducing the DPAs' workload.

- **Compliance.** Certifications may result in improved outcomes and more effective compliance on the ground due to the certification process, therefore reducing the enforcement burdens of DPAs.

- **Reduce complaint handling.** Because certifications may include complaint handling and dispute resolution mechanisms, they can help reduce DPAs' involvement in resolving individual complaints. This aspect of certifications will be important in practice, given that the GDPR gives DPAs a significant complaint-handling role.

- **Transparency.** Certification will require organisations to disclose their data practices in a transparent and organised fashion vis-à-vis the certification bodies and ultimately DPAs. This will make it easier for DPAs to properly assess these practices as well as possible violations of the GDPR. This, in turn, may drive down the costs and burdens of enforcement actions, both for DPAs and organisations.

2.4 Benefits for the Ecosystem and for Business Partners

The entire business ecosystem, including non-certified businesses, may benefit from certifications.

Because certifications signal a certain level of data protection and the presumption of GDPR compliance, certifications could streamline and shorten B2B due diligence and risk assessment processes between certified and non-certified organisations seeking qualified and trusted business partners in the digital ecosystem. This could lead to a greater speed of doing business and avoid protracted negotiations about privacy and security, benefiting business beyond just certified companies.

3. KEY POINTS AND RECOMMENDATIONS

3.1 GDPR Certification as an Opportunity

Certifications have significant potential as accountability and compliance mechanisms and for delivering privacy protection to individuals. For this potential to be realised, the following conditions must be fulfilled:

- **Promote benefits and incentivise businesses to adopt certifications.** Industry must be given the right incentives to take up certification instruments. This requires putting in place a certification process that is efficient and appropriately fast, scalable and affordable for all sizes of organisations. It also may include promoting the benefits of certifications by allowing certified organisations to transfer data outside the EU or to engage in broader data uses consistent with the GDPR and by recognising them as mitigation in enforcement and other interactions with DPAs. Otherwise, organisations will be reluctant to invest time and money in obtaining and maintaining certifications (in addition to the many other certifications to which they are already subject).

- **Certification granted to a company must also be stable and valid for at least three years** to avoid a constant cycle of re-certification at short intervals. The renewal of GDPR certifications after three years should be as easy and efficient as possible.

- **Emphasise features of building trust and a competitive advantage.** Certifications must be helpful and recognisable to individuals. Individuals must have trust in certifications and be able to rely on them in deciding with whom to do business, thereby providing certified companies or processes a competitive advantage vis-à-vis non-certified companies. In addition, certifications must be capable of engendering trust in the B2B context and provide a competitive advantage in that context as well.

- **Avoid one-size-fits-all.** Certifications should be adaptable, scalable to all sizes of companies and the nature of processing, and affordable without deviating from the core elements of the EU-wide GDPR baseline certification (discussed below at 3.3). This includes controllers and processors, large companies as well as SMEs, start-ups, etc. The adaptability and scalability would go to "how" these core elements are applied in the particular context and which elements may or may not be applicable at all.

- **Allow a variety of certifications.** The GDPR does not specify the object of certification, other than "processing operations" (Art. 42(1)) and "products and services" (Recital 100). In CIPL's view, consistent with the relevant GDPR provisions, the object of a certification can be a product, system or service, a particular process, or an entire privacy program[6] and information management infrastructure, or the full range of an organisation's products and services.[7] Limiting availability of certifications to only products, services or a technical process rather than an entire privacy program would seriously undermine the relevance, usefulness and thus

[6] Any certification of a privacy management program should be based on, or take into consideration as certification referentials, WP 155 BCR for controllers and WP 195 BCR for processors.

[7] Although the certification of DPOs has merits and may support the role of DPOs, we take the view that this specific certification falls outside the scope of Article 42 GDPR.

attractiveness of certifications. In any event, what is to be certified must be clearly articulated and distinguishable from non-certified products, processes, services or programs by and within an organisation. Consumer confusion must be avoided. Finally, not all products or services have to be certified at the same time, but different certifications within one organisation might be staggered.

- **Keep certifications technologically neutral.** Certifications should not be linked to any particular technologies, tools or frameworks that are prone to change over time. However, certifications should be technology-aware, in the sense that they take account of the impact of various technologies on personal data protection.

- **Certifications should reflect or be able to accommodate the latest developments.** Certifications should reflect or be able to accommodate up-to-date standards, current expertise and the most recent techniques. To accomplish this, certifications must be flexible enough to allow their application in contexts where technology and business practices evolve.

- **Benefit from existing certifications, including BCR and avoid bureaucratic and slow processes.** Because certification will normally require real effort and investment of resources from companies, it is important to find ways for organisations to benefit from existing certifications that are GDPR compliant, including Binding Corporate Rules (BCR). Companies will not want to start a process of "re-certification" at additional costs, if they have already been certified on the same or similar standards or requirements, but under a different name, or in different legal regimes or in different jurisdictions. Compliance with existing frameworks should be considered and recognised under the GDPR certification scheme. In short, certifications under the GDPR should not lead to another layer of bureaucracy. (See also discussion of BCR in 3.6 below.)

- **Learn lessons from the BCR approval process**. Lessons that need to be learned include, for example, the slow uptake by companies that may be associated with lengthy and costly processes.

3.2 Relationship between certifications, seals and marks

The GDPR does not specify a difference or relationship between certifications, seals and marks.[8] Indeed, the three concepts are not typically seen as something different but as co-equivalents.

CIPL believes that future work on GDPR certifications, seals or marks should not introduce unwarranted and unnecessary differentiation between these terms. However, it should be explored whether different elements of the certification process can be separated and performed by different actors. Possibly, certain actors could deliver parts of, or intermediate steps towards, a certification, seal or mark that is ultimately issued by a certification body or a DPA.

3.3 The need for one EU baseline certification

To ensure effectiveness and take-up of certifications, CIPL recommends the following:

[8] Certifications, seals and marks are not equal to icons, a transparency tool provided for in Article 12 GDPR. However, they may have a logo, mark or symbol that signifies them, just like an icon may signify a certain privacy or information management and use practice.

- **Preference for one EU baseline certification for all contexts and sectors, with possible differentiation in its application.** Ideally, there would be one baseline EU-wide certification standard—the "common certification" or "European Data Protection Seal" under Article 43(5) of the GDPR—developed under the lead of the Commission or the EDPB in collaboration with certification bodies and industry.

    - This standard or common certification should contain a comprehensive set of certification criteria that are both sufficiently granular and comprehensive to provide for EU-wide consistency and sufficiently high-level and flexible to allow for sector-, industry- and context-specific adaptation and application by certification bodies.

    - This standard or common certification may subsequently be applied taking account of the specific nature and complexity of the specific certifying company, product, service, process or whatever the object of certification might be. Not all the requirements necessarily come into play with each process or organisation. A less complex process or a smaller company may trigger the application of a more limited number of elements of this baseline certification. For example, a processor's certification might focus primarily on the data security elements and omit aspects of the certification not relevant to it.

    - As to differentiation in applying this baseline EU-wide certification between industry sectors, specialised certification bodies (or sophisticated, non-specialised certification bodies that have expertise with multiple or all industries) could specify this baseline certification to the needs, practices and circumstances of a particular industry sector. Approved sector-specific codes of conduct could be one mechanism to facilitate the sectoral-application of a baseline certification standard.

    - CIPL believes that creating separate sectoral or national certifications without reference to a general baseline EU-wide certification may be confusing, inefficient and unnecessary. Existence of a general comprehensive certification standard would enable specialised application and adaption of that baseline to specific sectors, such as pharma, advertising, credit referencing, etc.

    - The GDPR does allow national and EU-wide certifications to work in parallel. However, certifications that currently exist in the EU at the national level (or may exist in the future) should be aligned with this common EU-wide GDPR certification, including GDPR certifications that may already be under development in member states.

    - It is paramount to avoid an overlap and proliferation of certifications and seals in the EU (or elsewhere) as this could lead to confusion for all stakeholders, including individuals, and disencourage organisations from seeking certification altogether.

    - National certifications should be used only for organisations whose privacy programs, services and products are limited to a single member state. These national certifications should not only be issued in full compliance with Art 42(5), but before they are issued, it should also be ensured that they are consistent with each other and the general EU certification. Otherwise, there will be confusion for individuals and businesses moving and operating across the EU.

- There should be a mechanism for companies that are certified at the member states level to have that certification recognised in additional member states and also at the EU level. The Commission is encouraged to use its powers under Art 43(8) and (9) to set up such a mechanism. The EDPB can also set up mutual recognition process for national certifications.

3.4 Certification and compliance

- **Certification as an element of compliance and presumption of compliance** GDPR certification does not necessarily demonstrate full compliance with the GDPR, but it is one of the elements of demonstrating compliance and accountability. However, this one element[9] of compliance should be understood as a strong presumption that a certified product, process or an organisation's privacy program is in compliance. Thus, DPAs should publicly affirm and support the notion that certifications will be treated as a recognised and accepted means for demonstrating compliance. This is, of course, without prejudice to the DPAs' power to take action and enforcement against a certified organisation where there is a cause to do so and to review specific instances of possible non-compliance. It is essential for the success of certification that DPAs fully implement, recognise and honour the compliance function of certifications.

- **Certification could also go beyond compliance.** Certification is primarily an instrument for demonstrating GDPR compliance and should not exceed the requirements set forth in the GDPR. However, certification can also be used to show proactive and enhanced accountability above and beyond compliance. For example, consistent with the certification requirements, certified organisations may provide additional choices for individuals where possible and useful.

- **Certification should be a mitigating factor in the contexts of accountability and enforcement.** CIPL emphasises the importance of GDPR certification in the context of compliance and accountability, with focus on the issue of certification as a mitigating factor. DPAs should use the existence of certification as a mitigating factor in enforcement and when determining fines. DPAs should explicitly confirm this impact of certification to ensure better take-up in the marketplace.

- **Certification should be an aggravating factor only in exceptional cases**. If a certified organisation deliberately or with gross negligence chooses to ignore its certification commitments whilst gaining financial benefit from such certification, the certification may serve as an aggravating factor in an enforcement matter, or in establishing a fine.

- **Absence of certification should have no negative effect.** DPAs must make it clear that the absence of a certification should not result in a negative inference with respect to compliance. Having no certification should not be interpreted to mean that an organisation is less likely to be compliant. However, we acknowledge that there may be peer pressure in cases where one organisation in a sector gets certified for its product, service or compliance program. The rest of the market may follow for that reason alone. In addition, individuals may take note of who is certified and who is not.

[9] Art 24(3) GDPR.

- **Failure in receiving certification should have no negative effect.** Another issue relates to an organisation which applies for but fails to obtain a certification from the certification body or DPA. CIPL believes that being unsuccessful in receiving a certification from a certification body or generally withdrawing from the certification application process should not be reportable to a DPA, nor should it otherwise carry negative inferences with respect to compliance. However, it should be clear that this does not mean that an organisation that failed to certify with one certification body or DPA can then seek certification from another based on the same facts and program. Forum shopping must be avoided.

3.5 GDPR certification in relation to other relevant compliance instruments and frameworks

It is important to clarify the relationship between certification and specific accountability instruments and frameworks. Where possible, existing compliance tools should be integrated in the certification process.

- **Certifications must be consistent and take into account other instruments and frameworks, both within and outside EU**. Certifications based on ISO/IEC Standards, the EU-US Privacy Shield, the APEC CBPR and the Japan Privacy Mark are examples of other systems and frameworks having particular importance in this context. We must avoid unnecessary proliferation of different certification schemes or standards and we should use the GDPR process for creating certifications to harmonise, consolidate and make interoperable existing mechanisms, where possible. This requires an assessment of other data protection certifications already existing in the marketplace, in the EU and globally. Ultimately, companies will favour global schemes that are universally recognised.

- **GDPR certifications should have a streamlining effect**. Certifications should be used to streamline risk assessments, due diligence and contracting processes in B2B relationships (including controller/processors relationships). It should be recognised that GDPR certifications could be a considered in the context of risk assessments required by the GDPR, whereby a certified company, product or service would have a lower risk profile due to the certification.

- **GDPR certifications should not reinvent the wheel.** The functioning of GDPR certifications should be informed by lessons learned from other third-party privacy and security certification systems, such as the APEC CBPR and those based on ISO/IEC standards.

- **Codes of conduct are different instruments, but have similarities to certifications.** Codes of conduct are approved by the DPAs or provided general validity by the EU Commission. Also, they may include an ability to demonstrate adherence to the code similar to certifications. It should be elaborated how the two instruments relate to each other. It should also be considered how approved sector-specific codes of conduct can leverage certifications to support accountability and GDPR compliance in different sectors.

3.6 Certification and other instruments for data transfer, in particular BCR

CIPL notes that there are significant synergies between GDPR certification and BCR, a key instrument for data transfer which received additional recognition in Article 47 GDPR.

- **BCR are a de facto form of certification.** The two instruments are presented as separate concepts, but, arguably, BCR are a de facto form of certification and it makes sense to elaborate the similarities between the two concepts. BCR-approved companies and their executive leadership all regard their BCR as a de facto certification of their privacy compliance program and a "badge of recognition" by DPAs.

- **Recognise the assessments made in the BCR context.** BCR should be considered a specific type of certification. Thus, it should be explicitly recognised that BCR-approved companies may be given credit for their BCR towards GDPR certification in so far as their BCR meet the relevant certification criteria. (See also bullet on BCR in 3.1 above.)

- **Avoid additional re-certification costs.** The coexistence of the BCR and certifications in the GDPR should not lead to additional costs or investment of resources and efforts. That is why companies that have one of the two, should be able to leverage them for obtaining the other at no unnecessary additional cost.

- **Where a GDPR certification is deemed to provide adequate protection for international transfers, assess the relationship between that certification and other transfer mechanisms.** This assessment should in particular include the relationship with other data transfer mechanisms that work on the basis of a similar certification with which the EU schemes need to interact. This includes the EU/US Privacy Shield and the APEC CBPR.

- **Where a GDPR certification is deemed to provide adequate protection for international transfers, create interoperability with other transfer mechanisms**. CIPL recommends maximising the potential for GDPR certifications as cross-border transfer mechanisms. Thus, at a minimum, the development of a baseline certification standard should be recognised as a data transfer instrument, similar to the benefit offered by the BCR. Further, any new transfer-related certifications should, where possible, avoid creating conflicting requirements with other systems. In that connection, CIPL welcomes the Commission's interest in "explor[ing] [ways] to promote convergence between BCR under EU law and the Cross Border Privacy Rules developed by the Asia Pacific Economic Cooperation (APEC) as regards both the applicable standards and the application process under each system."[10] Of course, the same applies to "convergence" efforts between any new EU-based certification or codes and the APEC CBPR. We emphasise that many global companies have a single privacy management program, with all of its essential elements and substantive privacy requirements, that they apply consistently and comprehensively to their processing activities in all countries where they operate. They then leverage this same program to obtain Privacy Shield certification in the US, CBPR in APEC and BCR in Europe, under the respective approval and certification rules.

4. The roles of the various actors and recommendations

The GDPR provides roles to various actors in respect of certification. For instance, the Commission, DPAs and the EDPB all have roles in developing and drafting the standards or criteria for certification, but it is not evident who takes the lead. Also, the GDPR requires the member states, the DPAs, the EDPB and the

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

Commission to encourage the establishment of certification mechanisms. Here, it may be less crucial to lay down who takes the lead, but it would nevertheless be productive if these actors coordinate their efforts and develop a common approach. Regardless of who takes the formal lead, it is crucial that certification bodies and industry stakeholders participate in the development of the certification standards, criteria and mechanisms.

4.1 Member states

- Under the GDPR, (the governments of) member states must "encourage" certifications (Art 42(1)) and must ensure that certification bodies are properly accredited by a DPA or a national accreditation body. They should fulfil these roles under the GDPR in a proactive and consistent manner.

- It is key that member states encourage the certification and accreditation tasks in a coordinated manner, to ensure consistent approaches and avoid discrepancies between the implementation of these mechanisms in the member states.

- The member states' contributions to the delegated acts and the implementing acts (Art 43(8) and (9)) should be assessed in this perspective.

- At the national level, member states should encourage cooperation between DPAs and organisations in non-data protection domains that have experience in certification. Such cooperation should improve the quality and effectiveness of the GDPR certification processes.

4.2 DPAs

- **DPAs** have wide powers under the GDPR. Inter alia, they have the power to issue, renew and revoke certifications, or, where certifications are issued by certification bodies, the DPAs approve the accreditation criteria for such bodies. They also play a key role in the accreditation of certification bodies, which already exist in many member states.

- DPAs also have the power to disapprove or revoke individual certifications provided by certification bodies "where necessary". It should be further elaborated how this power will be implemented in a sensible way without introducing a new layer of review in each case. WP29 guidance should develop the appropriate criteria and a process for when and how to exercise this power, based on the notion that this power should be exercised only in exceptional cases.

- Equally, methods must be developed for DPA review of a third party's certification process, ex ante and/or ex post.

- The accreditation of certification bodies would be a new task for DPAs and does not necessarily fit within their past experiences. It also bears the risk of regulatory capture when the DPAs are required to take enforcement actions against companies, processes, products or services certified by a certification body which the DPA itself has accredited. The risk of regulatory capture is even more pronounced when the DPA itself issues certifications which it must later enforce.

- Thus, CIPL supports a co-regulatory approach with respect to certification, whereby certifications would primarily be provided by third-party certification bodies. (This approach would also help alleviate potential resource issues within the DPAs and potential bottlenecks in the certification process.

4.3 The EDPB (and WP29)

- The EDPB should agree with the Commission on who is in the best position to initiate an EU baseline certification.

- As mentioned, CIPL believes that, to ensure consistency, there should be one baseline EU-wide GDPR certification that would then be applied by different certification bodies (or DPAs) in different contexts. This baseline certification could be developed by or under the leadership of the EDPB or the Commission**.** Both the EDPB and the Commission are in the best position to encourage and ensure an EU-wide harmonised approach on certification.

- Before the EDPB will be effectively established, there is a role to play for the WP29. The WP29 should provide guidance at this stage, mainly on the issues addressed in the various parts of this paper. We encourage the WP29 to provide opportunities for the industry to give input before final issuing of guidance. In addition, the WP29 could start leading a process to develop a baseline GDPR certification, with input by relevant stakeholders, including industry.

- As concerns guidance, CIPL expresses a preference for the WP29's providing guidance at this timely stage over guidance by individual DPAs. This guidance should also encompass further defining the role of the lead DPA in EU-wide certifications.

4.4 The Commission

- The Commission should agree with the EDPB on who is in the best position to initiate an EU baseline certification.

- The GDPR gives the Commission a role to pass further implementing and delegating acts.[11] CIPL believes these provisions include the authority to develop a baseline EU-wide GDPR certification, and we recommend that either the Commission or the WP29 promptly commence that work, which includes seeking input from stakeholders.

- We recommend that the Commission clarify ambiguous elements of Art 43(8) and (9). More specifically, the Commission should clarify the meaning of (1) "specifying the requirements to be taken into account for the certification mechanisms"; (2) technical standards for certification mechanisms and data protection seals and marks"; and (3) "mechanisms to promote and recognise those certification mechanisms, seals and marks". The Commission should also explain how it seeks to put these provisions into effect.

[11] The Commission may adopt delegated acts for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms. (Arts 92 and 43(8) It may also adopt implementing acts to lay down technical standards for certification mechanisms and data protection seals and marks as well as mechanisms to promote and recognise such mechanisms, seals and marks. (Art 43(8))

- We believe the Commission's role under the GDPR includes ensuring the consistent implementation of certifications and seals in the EU, regardless of whether the Commission or EDPB takes the lead in drafting a baseline GDPR certification.

4.5 Certification bodies

- In general, for efficiency and scalability reasons, CIPL expresses a preference for third-party certification by certification bodies over certification by DPAs (see Art 42(5) GDPR). Certification by certification bodies avoids and alleviates potential resource issues and bottlenecks in the DPAs that could result from widespread use of certifications. It protects the DPAs' functional independence.

- Certification by certification bodies should be set up in a way that ensures an effective and practical participation of the private sector in the certification process. Further work is needed on defining how certification bodies and companies seeking certification will assign the risk between themselves that is associated with a potential DPA disapproval of a certification, such as losing the fee spent on the certification process. It should be established how the risks are divided under those circumstances.

4.6 National accreditation bodies

- National accreditation bodies have the task to accredit certification bodies (the same task is attributed to DPAs). To the extent accreditation is performed by national accreditation bodies as opposed to DPAs, such bodies must ensure that their accreditations of GDPR certification bodies are performed by staff with expertise in data protection and other related matters. This must ensure effective application of the GDPR accreditation criteria.

- The yet-to-be developed accreditation criteria that elaborate on the relevant GDPR requirements in Article 43(2) should be open to public comment and industry input before finalisation by the DPAs and/or the EDPB.

4.7 Private sector organisations

- Private sector organisations, including businesses that might seek certification and potential certification bodies, should have a meaningful role in the drafting and development of GDPR certification schemes and criteria. They are in the best position to advise on the potential impacts and practical implementation challenges that may be associated with specific certification criteria and standards.

- This means there should be a regular consultation with industry by member states, DPAs, the WP29/EDPB, the Commission and non-private sector certification and accreditation bodies, following structured consultation procedures. It also means that private sector organisations should have a proactive approach, taking up signals received in the market.

Appendix I -- Summary of GDPR Certification Provisions

I. Certification in the framework of Article 42 GDPR

Member states, DPAs, the EDPB and the EU Commission must encourage establishment of certifications: (Art 42(1),(3)); see also (57(1)(n); (70)(1)(n)).

- At national and particularly at EU level
- For use by controllers and processors
- Voluntary and available through a transparent process

Controllers and processors may use certifications: (Art 42(1),(2); see also (46(2)(f)); (Articles 24(3) and 28(5))

- As an element to demonstrate compliance with the Regulation
- As an element to demonstrate compliance with the obligations of the controller
- Demonstrate sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation (processor)
- Demonstrate appropriate safeguards in third countries for data transfers; certifications must be coupled with enforceable commitments by the controllers or processors in the third country to apply such safeguards

Certification does not reduce GDPR compliance obligations or prejudice the tasks and powers of the DPAs: (42(4))

- But it is one factor that DPAs must take into account in determining administrative fines—it can be both mitigating and aggravating (83(2)(j)(k))

Certifications are issued by certification bodies or the DPA: (42(5); see also 57(1)(o); 58(1)(c) and (2)(h); 58(3)(f))

- On the basis of criteria approved by the DPA (national) or the EDPB (EU DP seal)
- Last up to three years and are renewable (42(7))
- Can be withdrawn by certification bodies or DPAs, if the certification requirements are not or no longer met
- EDPB maintains a publicly available register of all certifications, seals and marks (42(8)); see also 43(6); 70(1)(o))

To obtain certification from a certification body or DPA, organisations must: (42(6))

- Provide all relevant information about the processing activities they seek to certify
- Provide access to these activities

The Commission's role: (43(8)); (43(9)); see also Art 92, on the exercise of delegation

- May adopt delegated acts to specify the requirements for the certifications (43(8)); see also Art 92, on the exercise of delegation
- May adopt implementing acts laying down technical standards for certifications and mechanisms to promote or recognise certifications

II. Certification bodies in the framework of Article 43 GDPR

Certification bodies issue, renew and withdraw certifications: (43(1))

- Must have an appropriate level of data protection expertise
- DPAs have the power to disapprove or revoke individual certifications provided by certification bodies "where necessary" (See also 58(2)(h))
- Responsible for the assessment leading to certification or withdrawal of certification (43(4))
- Must provide to the competent DPAs the reasons for granting or withdrawing certifications (43(5))

Must be accredited by DPAs and/or national accreditation bodies: (43(1)(a) and (b), 43(3), 43(4); see also 64(1)(c); 57(1)(p); 70(1)(p))

- For a maximum of 5 years
- On the basis of accreditation criteria approved by the DPA or the EDPB
- (Separate requirements in the case of accreditation by a national accreditation body) (established according to Regulation 765/2008 (Accreditation Regulation))
- DPAs and EDPB must make public the accreditation criteria for CBs (and certification criteria) (46(6); see also 42(8) and 70(1)(o))
- The DPA or national accreditation body can revoke the accreditation of a CB (43(7))

Conditions for accreditation of CBs: (43(2))

- Demonstrate independence and expertise
- Undertake to respect the approved certification criteria

- Establish procedures for issuing periodic review and withdrawal of certification
- Establish transparent complaint-handling mechanisms
- Demonstrate absence of conflicts of interest

Appendix II -- Schematic Overview Certification Tasks and Actors

GDPR Certification Actors

Member States	DPAs	EDPB	Commission	Certification Bodies	National Accreditation Body	Private Sector Organizations
Encourage Certifications (42(1))	Encourage Certifications (42(1); 57(1)(n))	Encourage Certifications (42(1)); 70(1)(n)	Encourage certifications (42(1))	Issue/renew/withdraw certifications (42(5); 42(7); 43(1))	Accredit Certification Bodies (43(1)(b))	Draft/propose certification criteria and Mechanisms
Ensure that Certification Bodies are accredited (43(1))	Approve accreditation criteria for Certification Bodies (43(1)(b);(43(3); 64(1)(c); 57(1)(p))	Approve accreditation criteria for Certification Bodies (43(3)); 64(1)(c); 70(1)(p))	"lay down technical standards for cert. mechs. and mechs. to promote and recognize cert. mechs" (through implementing acts)(43(9)) [Create accreditation criteria for Cert. Bodies ?]			Provide input into creation of certification criteria
	Approve certification criteria (42(5); 43(2)(b); 57(1)(n))	Approve certification criteria (42(5); 43(2)(b)); 70(1)(q)(provide opinion to Commission)	Specify requirements for cert. mechs. (through delegated and implementing acts)(43(8) [Adopt certification criteria ?]			Become certified (and attendant tasks, such as providing information and access to Certification Bodies and enter into safeguards commitments with c-b parties) (42(6); 46(2)(f)
	Accredit Certification Bodies (43(1)(a); 43(7); 57(1)(q); 58(3)(e))	Accredit Certification Bodies (70(1)(o))				
	Publicize accreditation criteria and certification criteria (43(6))	Publicize in Register Certification Mechanisms (accredited certification bodies) and certified organizations in third countries (42(8); 43(6); 70(1)(o))				
	Issue/renew/withdraw certifications (42(5); 42(7); 43(1);57(1)(o); 58(1)(c) and (2)(h)); 58(3)(f))					

GDPR Certification Tasks

Encourage Certifications	Approve accreditation criteria for Certification Bodies	Ensure that Certification Bodies are accredited	Accredit Certification Bodies	Specify requirements for Cert Mechs and lay down technical standards for Cert Mechs and Mechs to promote and recognize Cert Mechs	Draft/Propose Certification Criteria/Mech	Approve/Adopt Certification Criteria/Mechanisms	Issue/renew/withdraw certifications to controllers or processors	Publicize accreditation criteria and certification criteria and mechs
DPAs (42(1); 57(1)(n))	DPAs (43(1)(b); 43(3); 64(1)(c); 57(1)(p))		DPAs (43(1)(a); 43(2); 43(7); 57(1)(q); (58)(3)(e)			DPAs (42(5); 43(2)(b); (57)(1)(n))	DPAs (42(5); 42(7); 43(1); 57(1)(o); 58(1)(c); 58(2)(h); 58(3)(f)	DPAs (43(6))
EDPB (42(1); 70(1)(n)	EDPB (43(3); 64(1)(c); (70)(1)(p);		EDPB (70(1)(o)			EDPB (42(5); 43(2)(b); 70(1)(q) (opinion to Comm.)		EDPB (42(8); 43(6); 70(1)(o)
Member States (42(1))		Member States (43(1))						
Commission (42(1);	Commission (through implementing acts) (43(9)) [?]			Commission (through delegated and implementing acts)(43(8) and (9)	Commission (through delegated or implementing acts) (43(8) and (9)) [?]	Commission (through delegated or implementing acts) (43(8) and (9) [?]; 92(3) and (5))		
	National Accreditation Bodies under Regulation (EC) No 765/2008 and specified technical rules (43)(3)		National Accreditation Body (43(1)(b))					
							Certification Bodies (with approval/input by the DPA) (42(5); 42(7); (43(1))	
					Private Sector			

Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy

CENTRE FOR INFORMATION POLICY LEADERSHIP WHITE PAPER

Bojana Bellamy
President

Markus Heyder
Vice President and Senior Policy Counselor

REVISED AND UPDATED EDITION
25 September 2017

2200 Pennsylvania Avenue
Washington DC 20037
202-955-1563

30 St Mary Axe
London EC3A 8EP
+44 20 7220 5700

Park Atrium, Rue des Colonies 11
1000 Brussels
+32 (0)2 643 58 00

www.informationpolicycentre.com

EXECUTIVE SUMMARY

This white paper by the Centre for Information Policy Leadership (CIPL) is directed at all policymakers and legislators who are drafting privacy laws that regulate and contain restrictions for cross-border transfers of personal data.

While an approach to cross-border data transfers that relies on "accountability" for transferred data, rather than transfer restrictions, is both viable and preferable, an increasing number of countries are still including cross-border transfer restrictions modeled on the EU example. Given this trend, it becomes essential to ensure consistency and convergence and build on existing and accepted business and regulatory practices to enable benefits from cross-border data flows while ensuring protection from harms and risks for individuals. Therefore, privacy laws that do contain cross-border data transfer restrictions should also include the full range of existing and accepted exceptions and derogations to such restrictions, as well as a comprehensive set of available cross-border transfer mechanisms to enable accountable global data flows despite any transfer restrictions. These mechanisms include:

1) Contracts: The law should allow cross-border transfers on the basis of contractual arrangements that stipulate appropriate data privacy and security controls to be implemented by the organizations, thus establishing sufficient levels of protection for data leaving the jurisdiction.

2) Corporate Rules: The law should allow cross-border transfers based on binding corporate rules that provide for uniform and high-level protection and privacy compliance by all local entities of a multinational group.

3) Cross-Border Rules: The law should allow for enforceable corporate cross-border privacy rules modeled on the APEC Cross-Border Privacy Rules (CBPR).

4) Codes of Conduct, Certifications, Privacy Marks, Seals and Standards: The law should allow for the use of certified codes of conduct, certifications, privacy marks, and seals and standards as cross-border transfer mechanisms.

5) Self-Certification Arrangements: The law should allow the possibility of cross-border transfers based on negotiated arrangements, including arrangements that rely on "self-certification" to a given privacy standard, coupled with enforcement (such as EU-US Privacy Shield).

6) Consent: The law should allow cross-border data transfers on the basis of the data subject's consent.

7) Adequacy and Whitelists: The law should allow adequacy rulings and "whitelists."

8) Other grounds for transfer or derogations or exceptions to transfer restrictions, including: consent; necessity for the performance of a contract; public interest; establishment or defense of legal claims; vital interests; public register information; and legitimate interest.

Any derogations and exceptions to cross-border data transfer restrictions should be comprehensive in light of global practice.

Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy

A White Paper by the Center for Information Policy Leadership (CIPL)[1]
(Revised and Updated**)**

25 September 2017

I. Introduction

Legislatures in many countries currently are drafting or amending data protection laws. Often, these drafts and amendments attempt to regulate cross-border data transfers by imposing restrictions on transfers of personal data to other countries that do not have similar data privacy laws. Sometimes they also include so-called data localization provisions that require data or copies of data to remain in the country of origin. Yet, global data flows are the product of the increasing globalization and digitalization of business processes and society. They are foundational to the modern digital economy. The ability to use, share and access information across borders stimulates innovation, enables data-driven products and services, fuels economic growth and ideas, and is often the lifeline for remote communities. Any limitation on cross-border data flows, therefore, presents serious challenges to these key attributes and benefits of the global movement of data. This paper does not attempt to prove this particular point, however, as it has been discussed extensively elsewhere.[2] Instead, the paper enumerates important cross-border transfer mechanisms that should be included in any law that regulates or limits data transfers to other countries.

Initially, it should be noted that several significant countries with privacy laws, such as the United States, Canada and Mexico, do not impose material restrictions on cross-border transfers of personal information. From our perspective, these are not only viable but preferred models, particularly where organizations are required by legislation or jurisprudence to remain "accountable" for the continued protection of transferred data at the level it is protected inside the jurisdiction. Indeed, international privacy frameworks, such as the APEC Privacy Framework, also promote an approach based on accountability whereby businesses need to exercise "due diligence and take reasonable steps" to ensure that information remains protected wherever it travels and that recipient organizations will protect information at the original level.

---

[1] CIPL is a privacy and data protection think tank in the law firm of Hunton & Williams LLP and is financially supported by the law firm and 54 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 to ensure effective privacy protections and the effective and responsible use of personal information in the modern information age. 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] *See,* e.g. *Business Without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity*, US Chamber of Commerce and Hunton & Williams, 2014, available at https://www.huntonprivacyblog.com/files/2014/05/021384_BusinessWOBorders_final.pdf; *see also The Costs of Data Localisation: Friendly Fire on Economic Recovery,* European Centre for International Political Economy (ECIPE), 2014, available at www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.

A different model based on the EU data protection laws, however, is proliferating around the world. Under that framework, countries prohibit cross-border data transfers to other countries whose privacy laws are not substantially similar to their own and thus deemed not "adequate," unless certain specified derogations apply, or the transfers can occur under an exempted mechanism or recognized alternative transfer structures, which include concepts such as standard contractual clauses, binding corporate rules, cross-border privacy rules or bi- or multilateral cross-border transfer arrangements, such as the EU/US Privacy Shield Arrangement. Variations of this model containing differing selections of such derogations or mechanisms can now be found in numerous laws, proposed laws and other legal guidance around the world, including in Japan, Malaysia, Singapore, Brazil and Hong Kong.[3]

Given this trend, it is essential that there be greater convergence between the specific ways countries approach the regulation of data transfers. Indeed, there is already a well-established body of precedents and industry and regulatory best practices for data transfer mechanisms based on existing laws, regulatory guidance and organizational compliance programs. Moreover, global data flows and complex compliance strategies for the growing number of conflicting national requirements have become a key compliance priority for global organizations, and they have learned to deploy many and different mechanisms that enable the specific type of transfers and the particular jurisdictions involved. Accordingly, it is essential that countries legislating in this area take account of the existing and complex web of transfer mechanisms, laws and best practices that have evolved so that these mechanisms can work together and provide for seamless but still accountable global data flows that work for all kinds of cross-border data transfers, including transfers to or between controllers or processors and between affiliated companies or with third parties.

II. Data transfer mechanisms

We suggest that any legislator that has decided to include cross-border transfer restrictions in any data protection laws and regulations also include the following derogations, exceptions and alternative cross-border transfer mechanisms in such laws:

1. ***Contracts. The law should allow cross-border transfers on the basis of contractual arrangements that stipulate appropriate data privacy and security controls to be implemented by the organizations, thus establishing sufficient levels of protection for data leaving the jurisdiction.***

Contractual arrangements between transferors and transferees that establish legal obligations and the conditions under which data processing activities may take place are widely used by organizations globally, both for purposes of controller-to-controller transfers and, even more frequently, controller-to-processor transfers. They are an effective means to ensure that the legal obligations that attach to the

[3] *See* Japan's Act on the Protection of Personal Information, *available at* https://www.ppc.go.jp/en/legal/; Malaysia's Personal Data Protection Act of 2010, *available at* http://www.pdp.gov.my/images/LAWS_OF_MALAYSIA_PDPA.pdf; Singapore's Personal Data Protection Regulations 2014, *available at* http://bit.ly/1wdBTMb; Brazil's draft Law on the Processing of Personal Data, *available at* http://pensando.mj.gov.br/dadospessoais/english-information/; Hong Kong's Personal Data (Privacy) Ordinance (transfer provisions not yet in effect), *available at* http://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html. *See also* EU Data Protection Directive of 1995, *available* at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (and the proposed EU General Data Protection Directive).

data continue to apply as the data moves between countries, thereby ensuring a high level of protection of the data.

Because data flows occur within varying and specific business contexts, parties to a transaction must remain free to use contractual language that suits their specific business needs and information flows while also imposing the appropriate data privacy and security obligations applicable to the data. For example, the needs of businesses in the financial sector, health services sector, insurance sector and advertising sector vary greatly and each sector has unique business and regulatory needs that are best handled by contractual provisions customized to their situations and their data-handling needs.

Indeed, this context-specific flexibility in contracting is essential and thus we strongly discourage an approach that requires the parties to use non-modifiable standard contractual clauses for this purpose, as is currently the case with the EU standard contractual clauses.[4] Under that model, businesses are forced to have multiple contracts (one to meet their individual data processing needs and one merely to "tick-the-box" of privacy regulatory compliance), which is inefficient and ultimately does little to improve privacy protections. Rather, organizations should be able to adapt and tailor their contracts to the specific circumstances of the transfers to maximize both efficiency and privacy protections so long as they comply with and implement the relevant data protection requirements. This more flexible approach is evident in the privacy laws of countries such as Australia, Hong Kong and Singapore.[5]

Finally, some laws include pre-approval requirements for such contracts. For reasons of efficiency and resource management, regulatory or governmental review and pre-approval of the contracts should not be required. It is sufficient that the data privacy regulators or individuals have the ability to challenge noncompliance with data transfer requirements through appropriate legal processes.

2. Corporate Rules. The law should allow cross-border transfers based on binding corporate rules.

Another important cross-border transfer mechanism are corporate rules. An example of this concept are the EU's "binding corporate rules" (BCR). BCR are not mentioned in the current EU Data Protection Directive, but were developed by the EU's Article 29 Working Party (WP29) as a cross-border transfer mechanism consistent with the Directive's requirements.

Under that system, groups of corporate affiliates may transfer data to non-EU countries within their corporate group if the group has a set of rules, or BCR, that have been approved by a EU data protection

[4] The EU "standard contractual clauses" for transfers between EU controllers and foreign controllers or foreign processors have been widely used by organizations doing business in or with Europe. However, the EU standard contractual clauses cannot be modified and must be used as published. This will continue to be true under the EU General Data Protection Regulation (GDPR) that will come into effect on May 25, 2018.

[5] Australia Privacy Act 1988, Australian Privacy Principle 8, included in schedule 1 of the Privacy Act 1988, *available at* https://www.oaic.gov.au/privacy-law/privacy-act/; Hong Kong Privacy Ordinance, *available at* http://www.blis.gov.hk/blis_pdf.nsf/CurAllEngDoc/B4DF8B4125C4214D482575EF000EC5FF/$FILE/CAP_486_e_b5.pdf; Hong Kong Office of the Privacy Commissioner Guidance Note, *available at* https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_crossborder_e.pdf; Singapore Personal Data Protection Commission, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, The Transfer Limitation Obligation (Chapter 19), paragraphs 19.2 to 19.6, *available at* https://www.pdpc.gov.sg/legislation-and-guidelines/advisory-guidelines/main-advisory-guidelines - AG1.

authority. These BCR establish uniform internal rules for transferring personal data across the corporate group based on the EU data privacy requirements, and are binding on all relevant entities and personnel in the group. BCR exist both for organizations acting as controllers and as processors. The EU GDPR, which will come into effect in May 2018, explicitly includes BCR and expands their potential application from use only within a corporate group to a group of enterprises "engaged in a joint economic activity."[6] The term "engaged in a joint activity" is not defined in the GDPR and could be interpreted broadly. However, regardless of the meaning in the EU context, ideally, the scope of application for any type of BCR should mirror that of the APEC Cross-Border Privacy Rules (CBPR) (*see* discussion below), which do not have "within-group" or "joint-economic-activity" limitations. In other words, it should be possible for two BCR-approved companies to share data between themselves, based on the fact that both have approved BCR and provide for an adequate and high level of privacy protection and a comprehensive privacy program.

BCR also require a comprehensive privacy program and compliance infrastructure, including governance mechanisms, data protection officers (DPOs), policies and procedures, training and communication, audits and assessments and, in general, follow the essential elements of accountability and corporate compliance programs.[7] Thus, corporate rules like the BCR are, in essence, an accountability mechanism, which ensures compliance with local law, as well as adequate protection for data transferred across borders. As such, they should be implemented more widely, especially in light of similar accountability mechanisms, such as the APEC CBPR, with which corporate rules could be made interoperable (*see* below).

To ensure wider uptake and scalability in the future, especially for SMEs, any corporate rules system should not require prior approval by a data protection authority. Instead, such corporate rules could either be self-certified or reviewed by a third-party "Accountability Agent" (*see* CBPR section below), as appropriate, and, with respect to government or regulatory oversight, companies that employ such corporate rules should stand ready to demonstrate their compliance on request.

3. ***Cross-Border Rules. The law should allow for enforceable corporate cross-border privacy rules modeled on the APEC Cross-Border Privacy Rules (CBPR).***

We encourage the inclusion or recognition of cross-border transfer mechanisms such as the APEC CBPR developed by the Asia-Pacific Economic Cooperation (APEC) forum. The CBPR are an enforceable corporate code of conduct or certification mechanism for intra- and intercompany cross-border data transfers that have been reviewed and certified by an approved third-party certification organization

---

[6] *See* Art. 47(1)(a) GDPR.

[7] For more information on the essential elements and types of accountability, *see* CIPL white paper "Protecting Privacy in a World of Big Data, Paper 1, The Role of Enhanced Accountability in Creating a Sustainable Data-driven Economy and Information Society," http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_1_the_role_of_enhanced_accountability_21_october_2015.pdf; *see also* CIPL's earlier white papers and materials on accountability, http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/accountability-a_compendium_for_stakeholders__march_2011_.pdf;
Canada's "Getting Accountability Right with a Privacy Management Program," *available at* https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp; and Hong Kong's Privacy Management Program, *available at* https://www.pcpd.org.hk/pmp/pmp.html.

(Accountability Agent) in the jurisdiction in which the company is headquartered. The CBPR's objective is to uphold privacy protections to the standard embodied in the APEC Privacy Framework, a statement of privacy norms endorsed by the APEC forum in 2005. Enforcement of the CBPR is provided by APEC data protection and privacy authorities that have joined the APEC Cross-border Privacy Enforcement Arrangement (CPEA). APEC has also developed a corollary system for processors, called the APEC Privacy Recognition for Processors (PRP).

The advantage of this system is that it allows transfers not only within a global corporate group (or within a group of enterprises engaged in "joint economic activity") (such as under the BCR), but also between unaffiliated companies and to companies that are not CBPR-certified anywhere in the world. The CBPR-certified company remains liable for the protection of the information at the level of the originating APEC country and the CBPR, regardless of where or to whom the data is transferred.

Non-APEC countries that adopt similar mechanisms could make their cross-border rules mechanisms interoperable with the CBPR (and other similar schemes) if and so long as there is substantial overlap in the data protection requirements within each system. This will have the effect of creating a global certification mechanism requiring only one approval process. Creating transfer mechanisms with global applicability would be a significant efficiency gain to multinational and global businesses, and would also help regulators and, ultimately, benefit individuals.

Importantly, by way of exploring the viability of this goal, an effort was started between APEC and the EU's WP29 in 2012 to streamline the CBPR/BCR certification and approval processes when companies seek "dual certification" under both systems. Now, with the enactment of the GDPR, this EU/APEC collaboration also includes the EU Commission and has broadened its exploration of interoperability with the CBPR to include not only EU BCR, but also, and possibly primarily, GDPR certifications and, down the road perhaps, GDPR codes of conduct. This effort to create interoperability could serve as a model for similar efforts between other regions and transfer mechanisms.

4. ***Codes of Conduct, Certifications, Privacy Marks, Seals and Standards. The law should allow for the use of certified codes of conduct, certifications, privacy marks, and seals and standards as cross-border transfer mechanisms.***

Mechanisms related to corporate rules, BCR and CBPR, include codes of conduct, certifications, and privacy marks and seals (as envisioned, for example, by the EU Data Protection Directive and the EU GDPR), and international standards, such as the ISO standards. EU GDPR specifically encourages development of codes of conduct, certifications and seals and their use as data transfer mechanisms.

All of these mechanisms also impose substantive privacy requirements on organizations and are externally certified and enforceable. Any privacy law with data transfer restrictions should allow for the use of such mechanisms to enable accountable cross-border data transfers, in the same way BCR and CBPR currently enable them and as GDPR certifications and codes of conduct will in the future.[8]

[8] For a detailed discussion of certifications, see CIPL's white paper "Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms," April 2017, *available at* http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf.

5. ***<u>Bilateral or Multilateral Self-Certification Arrangements</u>. The law should allow the possibility of cross-border transfers based on negotiated bi- or multilateral arrangements, including arrangements that rely on "self-certification" to a given privacy standard, coupled with enforcement (such as EU/US Privacy Shield).***

Privacy laws that have cross-border transfer restrictions should also not preclude the option to develop bi- or multilateral frameworks and self-certification arrangements. The EU/US Privacy Shield Framework is one example. Under that framework, the US and EU negotiated a set of privacy principles for cross-border data transfers from the EU to the US to which US companies may "self-certify." Once a company self-certifies to the Privacy Shield, compliance with these privacy principles becomes binding and enforceable. Developing variations of this bilateral accountability model should be an option under any privacy law that contains data transfer restrictions. It would provide relevant authorities the flexibility to create data transfer frameworks that are particularly suited for SMEs and for contexts in which third-party certification may be impracticable and unnecessary.

6. ***<u>Consent</u>. The law should allow cross-border data transfers on the basis of the data subject's consent.***

As is already the case under many laws, consent should remain one of the options for legitimizing data transfers to other countries. Of course, such consent should be limited to appropriate circumstances where obtaining prior consent is practicable and meaningful and individuals have a real choice. (*See also* Section 8 below.)

7. ***<u>Adequacy and Whitelists</u>. The law should allow adequacy rulings and "whitelists."***

A "whitelist" is a list of jurisdictions to which cross-border transfers have been pre-approved on the basis of that country's privacy laws' purported "adequacy" under the standards of the evaluating country. The EU pioneered this legal basis for data transfers, and it is gaining some ground in other jurisdictions. While we do not believe this is a particularly practical or effective way to deal with global data privacy challenges and data flows (especially, given the long and onerous review process), these mechanisms may be useful in some contexts. Certainly, an individual assessment of the "adequacy" of every other country's privacy regime is unrealistic and risks becoming immediately obsolete due to changing circumstances on the ground. Even if such a task were achievable and the necessary expertise and language skills available, the theoretical legal "adequacy" of a particular regime does not address issues such as actual compliance, enforcement or enforceability in the evaluated jurisdictions. Nevertheless, where the relevant country assessments can be accomplished, "whitelists" and "adequacy" findings should be possible, provided that these transfer mechanisms are merely one of many available by law.

Similarly, such "whitelists" and "adequacy" findings could be applied to specific industries and sectoral laws in other countries (such as to transfers to processors, or outsourcing or cloud providers), keeping in mind that the same issues remain in terms of these mechanisms' practicability and effectiveness as a broad solution to regulating and enabling global data flows. Nevertheless, with this caveat, this option should be available too, if it is one of many. Note that an example of a sectoral application of "adequacy" can be found in the GDPR. This option recognizes that specific industry or business sectors regulated by separate laws may be subject to privacy or data protection requirements that provide adequate protection for international data transfers from the perspective of the evaluating country.

8. ***<u>Other Grounds for Transfer or Derogations and Exceptions</u>. The law should include other grounds for transfer or certain standard derogations or exceptions to data transfer restrictions that permit cross-border transfers. Data users should be able to rely on applicable derogations and exceptions without prior regulator review or permission.***

Many privacy laws already include standard derogations or exceptions to their cross-border transfer restrictions. Some of the most frequently used derogations allow transfers where:

- the transfer is necessary for the performance of a contract between the data subject and the controller or between the controller and a third party and (i) is entered into at the request of the data subject or (ii) is in the interest of the data subject;
- the transfer is for the purpose of legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights;
- the transfer is necessary in order to protect the vital interests of the data subject;
- the transfer is necessary for a legitimate interest of the controller or a third party that is not outweighed by the fundamental rights or freedoms of the data subject;
- the data subject has consented to the transfer;
- the transfer is necessary for reasons of public interest;
- the transfer is necessary to protect the vital interests of the data subject or of other persons; and
- the transfer is made from a public register.

This list is not comprehensive and may include additional grounds, derogations or exceptions. When drafting privacy legislation that contains transfer restrictions, it is advisable to make the list of transfer grounds, derogations or exceptions as inclusive and comprehensive as possible, taking into account, at a minimum, all grounds, derogations and exceptions that exist in comparable laws in other countries.

III. Further Recommendation

We specifically suggest that the following should *not* be included in provisions regulating cross-border data flows.

1. ***<u>Notification, Registration and Pre-Approval of Data Flows</u>. The law should <u>not</u> require that the Data Protection Authority be notified of a cross-border transfer, or that proposed categories of cross-border transfers be registered with or approved by the Data Protection Authority.***

While, historically, some laws contain such requirements, the trend is moving away from this approach (including the EU GDPR), as it is cumbersome and does not enhance privacy compliance. Many countries now realize that these requirements do not add much to the actual protection of individuals on the

ground. Also, given the prevalence and volume of global data flows, technology and processes, the enormous administrative burden and costs they impose both on organizations (especially SMEs) and on data protection authorities are not justifiable.

Summary

To conclude, if a legislature or regulator is to establish cross-border data transfer restrictions, it should also establish appropriate and effective exemptions so that necessary cross-border data transfers can continue while protecting the data and privacy of individuals. There are numerous available mechanisms and legal bases to facilitate such accountable transfers while still protecting individual privacy; and all of them should be included in any privacy law. Which one of them is appropriate for a given transfer scenario will depend on the context. Industry should be given flexibility in choosing which mechanism or legal basis works best under the circumstances and within the confines of appropriate accountability mechanisms and enforceability by the responsible authorities. Unnecessary government involvement should be avoided, as this imposes administrative and cost burdens on government and industry alike. Finally, accountability-based mechanisms that ensure effective and real protection for individuals, such as BCR, CBPR and similar mechanisms, should not only be an option, but specifically encouraged and incentivized.

For more information, please contact Bojana Bellamy, bbellamy@hunton.com, or Markus Heyder, mheyder@hunton.com.

CROSS-BORDER DATA TRANSFER MECHANISMS

25 September 2017

2200 Pennsylvania Avenue
Washington DC 20037
202-955-1563

30 St Mary Axe
London EC3A 8EP
+44 20 7220 5700

Park Atrium, Rue des Colonies 11
1000 Brussels
+32 (0)2 643 58 00

www.informationpolicycentre.com