EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE and CONSUMERS

Directorate C: Fundamental rights and rule of law
Unit C.3: Data protection

Brussels, 14 March 2019
DG JUST.C3

QUESTIONS TO PREPARE THE STOCK-TAKING EXERCISE OF JUNE 2019 ON THE APPLICATION OF GDPR

The European Commission would like to gather feedback on the application of the GDPR in view of a stock-taking exercise to take place in June 2019. Please note that the report based on the feedback is intended to be made publicly available.

The input should be sent to: JUST-C3@ec.europa.eu

1. **General comments**
   a. Please explain what were the main issues experienced by the organisations you represent in complying with the GDPR.

Lack of Harmonisation Across the EU: Despite its legal nature and intention, the GDPR has not solved the fragmented privacy landscape in the EU Member States created under Directive 95/46/EC. As an EU regulation, the GDPR aimed to harmonise data protection rules across Europe. Having a single set of rules across the EU was a strong incentive for organisations to drive operational efficiencies and to offer uniform services and products across the EU Digital Single Market. The promise of harmonisation would also bring legal certainty for individuals in the EU, who are increasingly mobile and participating in cross-border transactions. While the GDPR does provide for a single set of rules to a degree, it fell short of its harmonisation aim. Firstly, Member States, in national laws implementing the GDPR, have made full use of the margin of manoeuvre provided by the GDPR and this has led to the creation of differing rules (e.g. age of consent, processing of sensitive and biometric data, scientific research, etc.). Secondly, national interpretation, guidance and enforcement by DPAs show that there are diverging views, priorities and approaches among DPAs (e.g. differing national lists of high risk processing requiring a DPIA). The EDPB could also play a more proactive role in driving true consistency in the way DPAs interpret and approach data protection rules, compliance and enforcement, and not just through the formal consistency procedure for cross-border processing.

Other Regulatory Bodies Ruling on Privacy Issues: Some regulators have started ruling on topics that are in the remit of DPAs. The GDPR regulates the processing of personal data and establishes that the authorities responsible for enforcement are the Data Protection Authorities (DPAs) under the supervision of the EDPB. However, some other regulatory bodies (such as competition authorities or consumer bodies) have made decisions regarding privacy and data protection issues, where the DPAs (and in cross-border cases the lead DPAs) should be the competent authorities. The EDPB and the DPAs should play a more proactive role in engaging with other regulators to clarify their areas of competence to avoid conflicting and inconsistent rulings.

One Stop Shop Mechanism Not Respected by DPAs: The One Stop Shop mechanism has not provided organisations with the benefits of interacting with a single regulatory interlocutor in the EU. There is still ambiguity over the functioning of the One Stop Shop and, in particular, as to whether organisations are able to benefit from a single regulatory interlocutor in the EU. In particular, local DPAs are not respecting the One Stop Shop mechanism as they are sending orders, requests for information, starting audits or imposing fines directly on establishments present in their territory without first involving the lead DPA appointed by the organisations.

GDPR's Territorial Scope Complexities: The complexity of the GDPR's rules on territorial scope has created a multitude of issues for organisations operating in the international digital ecosystem. The GDPR applies extraterritorially to organisations outside the EU that offer goods or services to, or monitor the behaviour of, individuals in the Union, by virtue of Article 3. There is a plethora of open issues leading to legal uncertainty

about the GDPR's territorial scope. They include the relationship between Article 3 and Chapter V of the GDPR relating to data transfers; the role of the Article 27 representative; whether certain temporary activities constitute the offering of goods or services or monitoring of behaviour, etc. In addition, the rules on the territorial scope of national laws implementing the GDPR within the EU are not clear and create compliance hurdles for organisations operating in and between different EU Member States.

GDPR Interactions with Sectoral Laws: The GDPR's promise to create a single and uniform set of rules for data protection across Europe has not been realised, due to inconsistencies in sectoral laws. Despite the comprehensive, risk-based and technology neutral approach of the GDPR, some sector specific laws regulating data use have been or are being adopted or proposed in Europe (e.g. the Payment Services Directive 2 (PSD2), the Clinical Trial Regulation (CTR), as well as the proposed ePrivacy Regulation (ePR)). It is vital that interaction with the GDPR is fully considered when new requirements for data use are introduced. The danger is that sectoral laws (either due to lack of understanding of the GDPR or inconsistent interpretation of the GDPR by other regulators) may undermine the GDPR as the single and ultimate authority on data protection rules in the EU. At this stage, there are some conflicting requirements and no clear rules as to which standard prevails and which authorities will be responsible for enforcing these laws. Even the guidance from the EDPB and national regulators attempting to clear up some inconsistencies has not resolved the challenges for organisations trying to navigate these complex and inconsistent rules. Such legal complexity especially impacts SMEs and start-ups, which do not have resources or access to top legal advice and experienced DPOs. General confusion for organisations around such laws creates risk reticence in terms of data use and may impact the development of new products and services in the EU.

Regulatory Burdens on DPAs triggering over reporting practices from organisations: Effective oversight and enforcement of DPAs through expanded regulatory powers in the GDPR has been obstructed by the requirement to address all complaints and an overly strict interpretation of data breach notification rules. Under the GDPR, data protection authorities are obliged to handle every complaint they receive, regardless of the risk level involved. This has led to a significant burden on regulators. They spend much of their time and resources in the role of complaint-handler and police officer rather than prioritising their activities based on risks and harms to individuals and focusing their regulatory resources on constructive engagement with organisations and thought leadership activities. In addition to an avalanche of complaints, there is fear that the DPAs are being overburdened with a large number of breach notifications, even when they do not meet the applicable risk or timing threshold. With a real risk of heavy fines, organisations tend to over report. As of May 2019, over 144,000 queries and complaints were made, and over 89,000 data breaches reported, to EU DPAs. (See 1 Year GDPR – Taking Stock, European Data Protection Board, 22 May 2019, available at https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en).

Not Fully Tech Neutral or Future-Proof: Although intended to be technologically neutral and future-proof, the GDPR is not entirely adaptable to new developments in the digital economy. The GDPR is a principles-based law designed to be future proof and adaptable to emerging technologies and new uses of data. However, several of its provisions (e.g. restricted grounds for processing sensitive data, compatible use, data minimisation, profiling, automated decision-making) and, importantly, their overly strict interpretation, may lead to tensions with artificial intelligence applications, developing biotechnology and blockchain. Even the controller and processor distinction is not adaptable to all scenarios where the roles are not clear or the distinction is not applicable (e.g. Blockchain public networks). In addition, the GDPR embeds the risk–based approach precisely to allow for consideration of risks and harms to individuals and to calibrate compliance based on these risks and harms. There is a general sense that the risk-based approach is often neglected in the official guidance from DPAs and the EDPB. Yet, it is this very approach that would allow the GDPR to stay future proof and continue to adapt to new technologies, especially where they are bringing real benefits for individuals and society at large (provided risks and harms are not severe or likely, or have been mitigated).

Too Much Focus on Consent and Narrowing of Other Processing Grounds: For the GDPR to serve as a modern privacy law, its consent requirements cannot be emphasised as the principal legal ground for processing, nor should the other legal bases be continuously construed narrowly. Despite the fact that there are six legal basis contained in the GDPR, none of which are privileged over the other, there is a general feeling among data protection practitioners, lawyers and DPOs that DPAs, lawmakers and policymakers in the EU place strong emphasis on consent as a more important legal basis. Legitimate interest, which in most cases provides even more protection than consent, has received less recognition. In addition, there is a perception that DPAs (either deliberately or inadvertently) keep on narrowing the interpretation of all the other grounds for processing. This

approach is unrealistic in our data driven society and economy and not in line with the GDPR either. Such emphasis on consent is further reinforced by some "GDPR myths" that have emerged in the marketplace and among the public (e.g. consent is always required for data processing). This forces organisations to revert to consent, even when that is not appropriate and creates consent fatigue for individuals. The consent requirements in the GDPR and their interpretation by the DPAs are also much more complex and stringent compared to other privacy regimes globally (e.g. no possibility for opt-out consent under any circumstances) and do not function well for many modern day data processing contexts and do not provide effective protection for individuals. Finally, the discussions on the ePrivacy Regulation have contributed to further confusion generally on the role of consent, especially as the ePrivacy Regulation risks becoming the pre-dominant rule of internet data use and "trumping" the GDPR.

Lack of Clarity and Consistency Regarding Risk Assessments: The DPAs have missed the opportunity to fine-tune the risk-based approach in data protection by promoting a clear and consistent approach to assessing risk. The risk-based approach is firmly enshrined in the GDPR and has been a welcome innovation of the regulatory regime. The GDPR has internalised risk assessment within organisations and they are performing them more frequently. However, the full promise of the risk-based approach has not been realised. There doesn't appear to be a clear and consistent approach to risk assessment. Also, DPAs don't seem to refer to the risk-based approach in their guidance and interpretation or first GDPR enforcement actions, nor do they seem to factor in the benefits of processing in such processes. Although the Working Party 29 Guidelines on risk have been welcomed, overall regulatory guidance to date has been largely unhelpful and fragmented (e.g. numerous national lists of when a DPIA is required has led to unrealistic and unmanageable expectations for organisations). There is a strong feeling that more dialogue and consensus has to be built between organisations and DPAs on how to identify, assess and classify different risks and harms to individuals stemming from data processing.

Unrealised Potential of Certifications and Codes of Conduct as a Compliance Tool to Demonstrate Accountability: The potential of GDPR certifications and codes of conduct to demonstrate accountability has not been realised. One year after the GDPR went into effect, the regime surrounding GDPR certifications and codes of conduct – which serve as tools for demonstrating organisational accountability – has still not been effectuated. Also, the expected scope of certifications appears unnecessarily limited and not in line with their full potential under the GDPR. For example, certifications are currently envisioned not to cover entire privacy management programs, thereby losing their potential value as comprehensive accountability mechanisms under the GDPR.

Many GDPR Transfer Mechanisms Not Yet Operational: The framework to use certifications and codes of conduct as transfer tools has not been developed and little progress has been made to expand or improve existing cross-border data transfer mechanisms. Despite the potential of GDPR certifications and codes of conduct to serve as data transfer tools, the framework to enable their cross-border functions has yet to be developed and such development appears remote. In addition, the 2010 standard contractual clauses are currently facing legal challenge and alternative clauses are not yet available, should the outcome of the Schrems II case invalidate this mechanism. Indeed, much of the 2010 standard contractual clauses are redundant or are in conflict with Article 28 of the GDPR and thus should be reworked as supplemental clauses for processor-importers regardless of whether the exporter is a controller or processor. This would address the current gap in mechanisms for processor to sub-processor cross-border transfers. The 2004 standard contractual clauses should be updated to include data sharing terms, regardless of the geographic location of the controller-importer. Furthermore, BCR were formally recognised in the GDPR and have the potential to expand to entities engaged in joint economic activity. Yet, no work has taken place to expand the use of BCR as a transfer mechanism between different companies, nor to link this important mechanism to accountability obligations under the GDPR or to certifications.

Unrealised potential of BCR to facilitate GPDR implementation: The BCR's true nature – being a form of certification – has not been recognised and thus not been leveraged for important global interoperability purposes. BCR are, at bottom, a certification of a comprehensive privacy program. However, EU DPAs have not recognised this and, as a result, are not able to fully leverage the BCR for purposes of creating interoperability tools and mechanisms between the BCR and other accountability/compliance/transfer certifications, such as the APEC Cross-Border Privacy Rules (CBPR), that would enable organisations to more efficiently become certified/approved in various global accountability schemes that have significant substantive overlap.

2. Impact of the GDPR on the **exercise of the rights**
    a. How have the information obligations (in Articles 12 to 14) been implemented? Has there been a change of practices in this respect?

Members have modified their privacy notices to include the information required by the GDPR and improved comprehension and transparency by using clear and plain language. Some have adopted a layered approach to increase efficiency for the data subjects, have included graphics and videos to clarify key concepts and make it more intuitive or have developed user facing tools and dashboards to make it more user-friendly. Others have worked with privacy experts and designers to ensure that the required information is delivered to the data subject in a meaningful manner and in accordance with the design of the product or service. Practices need to continue to evolve to ensure that information is delivered to data subjects with the right level or granularity, in a meaningful manner taking into consideration technological developments (AI, facial recognition, etc.)

    b. Is there an increase of requests (where possible provide estimates):

CIPL members generally report an increase in the exercise of rights and more detailed information requested by individuals. Figures and type of requests vary per sector.

        i. to access data?
        ii. for rectification?
        iii. for erasure?
        iv. to object?
        v. for meaningful explanation and human intervention in automated decision making?
    c. Are there requests on data portability?
    d. On which rights do these requests mostly relate to?
    e. Are there any difficulties in the application of the rights (by controllers, by DPAs), including for meeting the deadlines for responding to the requests?

Some CIPL members underline the difficulty to sometimes verify the identity of the individual, especially for requests outside of any customer relationship. In addition, CIPL members ask that the amount of time and resources necessary to answer some requests not be underestimated.

    f. What percentage of the requests was manifestly unfounded or excessive? Please describe why these requests were unfounded or excessive.

Some CIPL members report that rights of data subjects are sometimes being exercised in an excessive manner. For instance, disgruntled employees may request a copy of all their personal data to prepare their defence in the context of a HR lawsuit. Some individuals exercise their right of portability at the request of a competitor of the data controller under the promise of a more advantageous offer to the data subject. Finally, individuals sometime request information that the data controller does not collect or process.

3. Impact of Article 7(4) regarding the **conditions for valid consent** on your business model/consumers
    a. Are there any issues with the use of consent as legal basis for specific processing operations? (e.g. complaints received) When requesting consent, how did individuals respond?

In addition to creating consent fatigue for individuals when used too frequently, consent as a legal basis for processing does not function well for many modern day data processing contexts. Furthermore, some organisations receive many requests from individuals to withdraw their consent, including when the processing is based on another legal basis that does not enable retrieving of consent or objecting to the processing (contractual necessity, for instance).

b. Have organisations switched the legal ground for processing from consent to another legal ground?

Despite the fact that there are six legal basis contained in the GDPR, none of which are privileged over the other, there is a general feeling among data protection practitioners, lawyers and DPOs that DPAs, lawmakers and policymakers in the EU place strong emphasis on consent as a more important legal basis. Legitimate interest, which in most cases provides even more protection than consent, has received less recognition. In addition, there is a perception that DPAs (either deliberately or inadvertently) keep on narrowing the interpretation of all the other grounds for processing. This approach is unrealistic in our data driven society and economy and not in line with the GDPR either. Such emphasis on consent is further reinforced by some "GDPR myths" that have emerged in the marketplace and among the public (e.g. consent is always required for data processing). This forces organisations to revert to consent, even when that is not appropriate and creates consent fatigue for individuals. The consent requirements in the GDPR and their interpretation by the DPAs are also much more complex and stringent compared to other privacy regimes globally (e.g. no possibility for opt-out consent under any circumstances) and do not function well for many modern day data processing contexts and do not provide effective protection for individuals. Finally, the discussions on the ePrivacy Regulation have contributed to further confusion generally on the role of consent, especially as the ePrivacy Regulation risks becoming the pre-dominant rule of internet data use and "trumping" the GDPR.

c. How are businesses addressing the issue of tied consent? How are they distinguishing between contract as legal basis and consent?

CIPL Members underline the level of legal uncertainty surrounding the scope of the different legal bases for processing, including consent which is reinforced by the first enforcement cases. A more consistent EU approach is necessary.

4. **Complaints and legal actions**
   a. Are there any complaints against your organisation(s) submitted before DPAs?
   b. Are there any court actions against your organisation(s)?
   c. Are there any court actions against decisions, or absence of decisions, of DPAs?
   d. In all above cases, please explain what is the matter of the complaint or court action and for which types of infringements of GDPR?

5. Use of **representative actions** under Article 80 GDPR:
   a. Are you aware of representative actions being filed against your organisation(s) or in your Member State? As an organisation representing civil society, have you filed representative actions in any Member State?
   b. What types of representative actions (complaint to DPA or to court, claim for compensation)? In which country/ies?
   c. Against whom and for which types of infringements of GDPR?

6. Experience with **Data Protection Authorities** (DPAs) and the **one-stop-shop mechanism** (OSS):
   a. Are there any difficulty experienced in the dealings with DPAs (by individuals/businesses)?

There appears to be some conflicting expectations from the DPAs, in particular, as it relates to breach notification requirements.

b. Are there difficulties in obtaining advice or guidance material by the DPAs?

Some Members report a slow response time from DPAs when requesting guidance. There also appears to be a backlog in BCR file review and approval.

c. Are DPAs following up on each complaint submitted, and in a timely manner?

d. How many of your business members have declared a main establishment to a DPA and benefit from a Lead Authority? Have they experienced difficulties with the functioning of the OSS?

<u>One Stop Shop Mechanism Not Respected by DPAs</u>: The One Stop Shop mechanism has not provided organisations with the benefits of interacting with a single regulatory interlocutor in the EU. There is still ambiguity over the functioning of the One Stop Shop and, in particular, as to whether organisations are able to benefit from a single regulatory interlocutor in the EU. In particular, local DPAs are not respecting the One Stop Shop mechanism as they are sending orders, requests for information, starting audits or imposing fines directly on establishments present in their territory without first involving the lead DPA appointed by the organisations.

e. Do you have experience with the designation of representatives of controllers or processors not established in the EU?

f. Are you aware of guidelines issued by national DPAs supplementing or conflicting with EDPB guidelines? (please explain)

CIPL Members report difficulties in reconciling all national DPIA lists and in having a consolidated view of all the criteria that a company would have to consider when assessing whether a multi-country processing entails high risk.

7. Experience with **accountability** and the **risk-based approach**:

a. What is the feedback from your members on the implementation of accountability? And their experience with the scalability of obligations (e.g. Data Protection Impact Assessment for high risks, etc.)?

Organisational Accountability improved organisations' ability to build and implement accountable privacy management programs and demonstrate accountability internally to the Board and externally to regulators, customers, data subjects and shareholders, serving as a potential mitigating factor in case of enforcement. The GDPR's accountability requirement to comply with data protection principles and to be able to demonstrate such compliance has led to an increased uptake of implementing comprehensive privacy management programs, and to organisations revisiting existing programs to ensure they are up to date. Accountability drives more efficiencies at the organisational level and more effective and better protection for individuals and their data. By putting the burden on organisations handling data, both in the private and public sector, accountability also increases the overall trust in the digital information society and age.

Organisations welcome the flexible approach of the GDPR compared to the previous registration regime. The GDPR's ambition to enable scalability of obligations is, however, trumped by the lack of common standards among DPAs on key accountability elements (such as records of processing or high risk processing criteria for DPIAs), making it more difficult to find a scalable and reliable method to address all expectations in all jurisdictions.

As far as the risk-based approach is concerned, the DPAs have missed the opportunity to fine-tune the risk-based approach in data protection by promoting a clear and consistent approach to assessing risk. The risk-based approach is firmly enshrined in the GDPR and has been a welcome innovation of the regulatory regime. The GDPR has internalised risk assessment within organisations and they are performing them more frequently. However, the full promise of the risk-based approach has not been realised. There doesn't appear to be a clear

and consistent approach to risk assessment. Also, DPAs don't seem to refer to the risk-based approach in their guidance and interpretation or first GDPR enforcement actions, nor do they seem to factor in the benefits of processing in such processes. Although the Working Party 29 Guidelines on risk have been welcomed, overall regulatory guidance to date has been largely unhelpful and fragmented (e.g. numerous national lists of when a DPIA is required has led to unrealistic and unmanageable expectations for organisations). There is a strong feeling that more dialogue and consensus has to be built between organisations and DPAs on how to identify, assess and classify different risks and harms to individuals stemming from data processing.

a. What are the benefits/challenges of GDPR in your line of business?

As further detailed in CIPL's paper "GDPR One Year In: Practitioners Take Stock of the Benefits and Challenges", the GDPR has had the following benefits for organisations:

- Facilitated top-management focus, buy-in and increased resources for compliance;
- Shifted view of privacy law from compliance obligation to top business issue and business enabler, linked to organisations' data strategy and digital transformation;
- Improved organisations' ability to build and implement accountable privacy management programs and demonstrate accountability internally to the Board and externally to regulators, customers, data subjects and shareholders, serving as a potential mitigating factor in case of enforcement;
- Encouraged organisations to create a single privacy management program for their global operations and entities;
- Improved overall privacy awareness, data management and sharing tailored to company department specificities, informing important business decisions;
- Acted as a business enabler by giving the data privacy team a seat at the table and bringing business and privacy professionals closer together to discuss how relevant compliance issues align with business goals;
- Provided the organisation with an identified expert/team to oversee the privacy management program, implementation of GDPR requirements and ongoing compliance;
- Fostered good data hygiene, governance, management and traceability;
- Lowered data protection liability risk and supported internal business decisions;
- Promoted user-centric and innovative transparency, generating trust in organisations' data handling practices and strengthening relationships both within and outside of the organisation;
- Provided a competitive edge in B2B negotiations and improved ability for organisations to identify trustworthy service providers;
- Improved organisational processes to facilitate exercise of individual rights;
- Strengthened organisations' resilience to breaches and prepared them to respond more efficiently;
- Required organisations to understand that GDPR implementation and ongoing compliance are enterprise-wide processes, requiring multifunctional teams and a joined-up approach between different functions and leadership (CDO, CIO, CISO, CMO, DPO, Legal, Engineering, etc.)

As further detailed in CIPL's paper, the GDPR presents the following challenges for organisations:

- Despite its legal nature and intention, the GDPR has not solved the fragmented privacy landscape in the EU Member States created under Directive 95/46/EC;
- Non-data protection regulators have started ruling on topics that are within the remit of DPAs;
- The One Stop Shop mechanism has not provided organisations with the benefits of interacting with a single regulatory interlocutor in the EU;
- The complexity of the GDPR's rules on territorial scope has created a multitude of issues for organisations operating in the international digital ecosystem;
- The GDPR's promise to create a single and uniform set of rules for data protection across Europe has not been realised, due to inconsistencies in sectoral laws;
- Effective oversight and enforcement of DPAs through expanded regulatory powers in the GDPR has been obstructed by the requirement to address all complaints and an overly strict interpretation of data breach notification rules;
- Although intended to be technologically neutral and future-proof, the GDPR is not entirely adaptable to new developments in the digital economy;
- For the GDPR to serve as a modern privacy law, its consent requirements cannot be emphasised as the principal legal ground for processing, nor should the other legal bases be continuously construed narrowly;

- The DPAs have missed the opportunity to fine-tune the risk-based approach in data protection by promoting a clear and consistent approach to assessing risk;
- The potential of GDPR certifications and codes of conduct to demonstrate accountability has not been realised;
- The framework to use certifications and codes of conduct as transfer tools has not been developed and little progress has been made to expand or improve existing cross-border data transfer mechanisms;
- The BCR's true nature – being a form of certification – has not been recognised and thus not been leveraged for important global interoperability purposes.

b. What do you think the overall impact of GDPR will be on your organisation's approach to innovation?

Although intended to be technologically neutral and future-proof, the GDPR is not entirely adaptable to new developments in the digital economy. The GDPR is a principles-based law designed to be future proof and adaptable to emerging technologies and new uses of data. However, several of its provisions (e.g. restricted grounds for processing sensitive data, compatible use, data minimisation, profiling, automated decision-making) and, importantly, their overly strict interpretation, may lead to tensions with artificial intelligence applications, developing biotechnology and blockchain. Even the controller and processor distinction is not adaptable to all scenarios where the roles are not clear or the distinction is not applicable (e.g. Blockchain public networks). In addition, the GDPR embeds the risk–based approach precisely to allow for consideration of risks and harms to individuals and to calibrate compliance based on these risks and harms. There is a general sense that the risk-based approach is often neglected in the official guidance from DPAs and the EDPB. Yet, it is this very approach that would allow the GDPR to stay future proof and continue to adapt to new technologies, especially where they are bringing real benefits for individuals and society at large (provided risks and harms are not severe or likely, or have been mitigated).

CIPL Members also report tension between the GDPR and different global privacy laws that may slow product development cycles.

c. In which area did your organisation have to invest most in order to comply with the GDPR? How useful do you consider this investment for the overall performance of your organisation?

Members report investments in legal advice, consulting service and IT and security technologies.

The GDPR implementation has shifted the view of privacy law from compliance obligation to top business issue and business enabler, linked to organisations' data strategy and digital transformation. The GDPR enabled organisations and their senior leadership to position data privacy compliance as a business enabler, unlocking the potential for organisations to benefit from wider responsible data uses and data driven innovation. Data privacy has been linked firmly to business data strategy and goals, and serves as a competitive advantage.

The GDPR implementation also fostered good data hygiene, governance, management and traceability. The collective impact of several GDPR requirements meant that organisations had to be particularly thoughtful about the data they process. This includes the way they collect, use, share, secure and maintain data within the organisation and with business partners and providers. The obligation to maintain records of processing required organisations to review the data they hold (including customer and employee data), their existing products, services and business lines and the parties with which they share data. In line with the privacy by design principle, organisations also had to review and reassess the relevance and business need for data, in order to ensure data quality, accuracy and retention of only necessary data. Better data management meant not only knowing where and how data is used but maintaining documentation and evidence in relevant product and service processes, including data flow mapping.

d. To which extent could your organisation rely on existing technical and organisational measures or did you establish a new data management system?

Improved organisations' ability to build and implement accountable privacy management programs and demonstrate accountability internally to the Board and externally to regulators, customers, data subjects and shareholders, serving as a potential mitigating factor in case of enforcement. The GDPR's accountability requirement to comply with data protection principles and to be able to demonstrate such compliance has led to an increased uptake of implementing comprehensive privacy management programs, and to organisations revisiting existing programs to ensure they are up to date. Accountability drives more efficiencies at the organisational level and more effective and better protection for individuals and their data. By putting the burden on organisations handling data, both in the private and public sector, accountability also increases the overall trust in the digital information society and age.

The GDPR also encouraged organisations to create a single privacy management program for their global operations and entities. The GDPR has led to many organisations addressing data privacy not only for their EU operations, but also globally across all their business lines, products, services and locations (where appropriate, and taking variations in national law into account). By "putting their house in order", organisations are now dealing with a centralised, streamlined and calibrated privacy program. This enables operational efficiencies for organisations and more consistent protection for individuals.

e. Do your members experience an increase of awareness and of trust of their customers due to the implementation of technical and organisational measures to comply with the GDPR?

CIPL Members report an increase in awareness more specifically related to the transparency of their privacy practices.

The GDPR **promoted user-centric and innovative transparency, generating trust in organisations' data handling practices and strengthening relationships both within and outside of the organisation.** The GDPR transparency requirements required a deep dive into the data held by organisations to reach an unprecedented level of transparency both internally, for the organisation and externally to individuals, business partners and regulators. Many organisations modified, or in some cases even completely reinvented, how they engage with individuals to provide information in a more user-centric and design focused way. This created operational efficiencies around the use and accessibility of data within organisations, enhanced customer experience as well as generated external trust and engagement.

In addition, the GDPR provided a competitive edge in B2B negotiations and improved ability for organisations to identify trustworthy service providers. GDPR compliance is an asset in the context of negotiations with business partners who are more likely to deal with GDPR compliant companies in any transactions involving data exchange. This is especially apparent in the selection of processors, where management and security of client/customer data is of paramount importance to companies seeking to engage them. It also increases efficiency in the due diligence processes for selecting appropriate service providers and vendors. A survey of over 3000 senior companies' executives reported that GDPR compliant companies have "better speed to market", with shorter lead-time to negotiate agreements and savings on opportunity costs. (See Maximising the Value of your Data Privacy Investments, CISCO 2019 Data Privacy Benchmark Study, January 2019, available at https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf).

8. **Data protection officers** (DPO):

a. Did the organisations you represent designate a mandatory DPO pursuant to Article 37(1) GDPR?

Organisations have generally appointed mandatory DPO when meeting the criteria of Article 37(1). This ensured that certain organisations that traditionally did not have a designated member of staff responsible for data protection would integrate one into their organisational structure.

b. Did the organisations you represent designate a mandatory DPO pursuant to national law implementing Article 37(4) GDPR? Please specify which national law and for which situations.

c. Did the organisations you represent designate a DPO on their own initiative, without being required to do so by the GDPR or by national law?

Organisations that are not legally required to appoint a DPO have assigned responsibility for data privacy and engaged privacy professionals (whether a DPO or not) with relevant expertise to assist with GDPR compliance. Among other tasks, data privacy professionals have been reviewing proposed data operations, assisting with risk assessments, creating staff training programs and working with the CISO and security team on breach preparedness and response.

d. Did associations or other bodies representing categories of controllers or processors designate data protection officers?

e. What is the experience of the organisations you represent with the performance of DPOs?

The GDPR acted as a business enabler by giving data privacy teams a seat at the table and bringing business and privacy professionals closer together to discuss relevant compliance issues in line with business goals. In some organisations, the GDPR resulted in higher visibility of data privacy teams and led them to work cross-functionally with a greater variety of organisational departments. In some cases, this gave privacy teams better insight into business imperatives, how those departments work and the projects they are working on, including technical aspects. It resulted in data privacy teams strengthening their position as trusted business advisers and providing more practical, pragmatic and strategic advice on compliance and in the translation of GDPR requirements into actionable tasks in line with business goals.

In addition, DPO and privacy teams have been very helpful in raising privacy awareness across the company including at the C-Suite level. They have also significantly contributed to building accountability of the organisation through DPIA, incident management exercises and breach notifications, data subject request handling, DPA interactions and trainings.

9. Controller/processor relationship (Standard Contractual Clauses)

a. What is the experience of the organisations you represent on the adaptation of current contracts?

CIPL members generally report that the adaptation has been slow due to lengthy discussions between the parties on security measures, cost allocation of data breaches, extent of the new obligations of the data processor, and above all on liability and indemnification discussions. Members also highlight difficulties in updating contracts when the processor is outside of the EU and, as a consequence, not familiar with GDPR requirements.

b. Is there a need for the adoption of standard contractual clauses under Article 28(7) GDPR? Explain what are the main reasons.

CIPL considers that there is no need for the adoption of standard contractual clauses under Article 28(7). The wording of Article 28 GDPR is already prescriptive and provides a good standard baseline for controllers and processors to formulate contracts according to their specific sector, situation and relationship. In case the Commission were to decide to prepare such clauses, CIPL recommends that they be developed in an iterative process together with industry.

c. If standard contractual clauses were to be prepared, what elements and specifications should be included? (e.g. auditing, liability allocation, duty of cooperation, indemnification)?
d. Do you have suggestions in terms of how to ensure the "user-friendliness" of such standard contractual clauses?
e. In case you have drafting suggestions for specific clauses, please share.

10. Adaptation/further development of **Standard Contractual Clauses (SCCs) for international transfers**
    a. What are your practical experiences with the existing SCCs: Do they serve the purpose? If not, where do you see room for improvements? Have you encountered any problems in using the existing SCCs?

It appears that SCC have generally served their purpose and have been relied upon in commercial relationships extensively without issue, as they are commonly known by the different economic actors.

    b. Do you see a need to adapt the existing SCCs, generally and/or in the light of the GDPR? (e.g. different structure/design? additional safeguards? combination with Art. 28 standard contractual clauses for processors?)

Organisations would welcome solutions designed to reduce complexity (by ensuring consistency between the terms of the controller to processor SCCs and the terms of Article 28) while updating references and terminology in line with the GDPR. CIPL cautions, however, that any amendment to the SCCs need to be addressed pragmatically. For instance, updated SCCs should apply to future relationships only, but should not mandate for the updating of all currently signed SCCs. CIPL would also suggest reworking the 2010 standard contractual clauses as supplemental clauses for processor-importers regardless of whether the exporter is a controller or processor. This would address the current gap in mechanisms for processor to sub-processor cross-border transfers. The 2004 standard contractual clauses should be updated to include data sharing terms, regardless of the geographic location of the controller-importer.

    c. Do specific clauses require further clarification (e.g. auditing, liability allocation, duty of cooperation, indemnification)?

    d. Is there a need to adapt the SCCs in light of the *Schrems II* court case (concerning access by third country authorities), e.g. with respect to monitoring/reporting obligations on the data importer/exporter? Do you have suggestions on ways and means to strengthen the possible control by the data exporter vis-à-vis the data importer and the measures to enforce such control (e.g. not only suspending the transfer of data but actually recalling the data already transferred?) Do you have any other suggestions on how to further strengthen data protection safeguards and control mechanisms (including by the DPAs) with regard to government access?

e. Is there a need to develop new SCCs, e.g. for the processor/sub-processor relationship, joint-controllership, processor-to-controller relationship or specific processing operations?

There is a need for the adoption of SCCs to address the processor/sub-processor relationship as there is still a gap in the GDPR in terms of mechanisms for processor to sub-processor cross-border transfers.

As mentioned in answer to question 10(b), CIPL also suggests reworking the 2010 standard contractual clauses as supplemental clauses for processor-importers regardless of whether the exporter is a controller or processor. This would address the current gap in mechanisms for processor to sub-processor cross-border transfers.

f. Do you have suggestions in terms of how to enhance the "user-friendliness" of SCCs?
g. In case you have drafting suggestions for specific clauses, please share.

11. Have you experienced or observed any problems with the **national legislation** implementing the GDPR (e.g. divergences with the letter of GDPR, additional conditions, gold plating, etc.)?

The GDPR provides for more than fifty opening clauses and Member States have made full use of their margin of manoeuvre[1], which resulted in the creation of differing rules. As a result, controllers and processors face an additional layer of complexity for their operations in the EU to adapt their processing operations and products accordingly.

In addition, the rules on the territorial scope of national laws implementing the GDPR (including its opening clauses) within the EU are not consistent or clear and create compliance hurdles for organisations operating in and between different EU Member States. It appears that most Member States' laws apply a criteria equivalent to Article 3(1) GDPR,[2] while others apply criteria equivalent to Article 3(2) GDPR.[3] This may result in several laws applying to the same situation or even conflicts of laws within the EU itself.

[1] For example, Article 8 on Children's Age of Digital Consent, Article 35(4) permitting data protection authorities to define their own list of high risk processing operations warranting a DPIA, Article 37(4) permitting Member States to require the designation of a DPO in circumstances additional to the mandatory GDPR requirements, Article 88 on processing on the context of employment.
[2] Examples include Belgium, The Netherlands and Ireland.
[3] France, for instance.