Multi-stakeholder expert group to support the application of Regulation (EU) 2016/679

QUESTIONS TO PREPARE THE COMMISSION 2024 REPORT ON THE APPLICATION OF GDPR

Responses of Estelle Dehon KC (Barrister, Cornerstone Barristers, London, UK), Individual Member

1. General comments

a. What is your overall assessment (benefits/challenges, increase in trust and awareness, etc.) of the application of the GDPR since May 2018? Are there priority issues to be addressed?

Answer: The GDPR has facilitated significant positive changes in data protection and privacy and has set a global standard. Overall, data professionals are seeing an increase in compliance across many different types of organisation.[1] There are, however, still areas where improvements could be made to ensure that it remains effective and practicable. In particular, there remains a lack of confidence that organisations are complying with data retention (ie minimisation) requirements, and confidence in this areas is diminishing.

Benefits: Since it entered into force in 2018, the GDPR has enhanced data protection rights significantly. It has enabled individuals to gain more control over their personal data through the exercise of their rights. The right of access remains the most well-known and used of these rights, but other rights, such as rectification, erasure and data portability, are increasingly being exercised. Notably, the GDPR has also significantly raised awareness among organisations and individuals about data protection and privacy rights. Organisations (including government agencies) are now more accountable for data protection, with obligations to implement data protection principles and document compliance.

Furthermore, the GDPR has gone a long way towards harmonising the relevant rules across the EU, simplifying the regulatory environment for international business. It has done this while driving improved data security. In particular, mandatory data breach notifications have led to a greater emphasis on data security, data minimisation and prompt responses to data breaches.

[1] See the surveys published by the UK Data Protection Index, launched at the end of July 2020: https://www.dpocentre.com/resources/uk-data-protection-index/.

Challenges: The main area that DPOs identify as a challenge (ie an ongoing concern because of lack of compliance) is data retention and proper application of retention periods. Retention – meaning ensuring that personal data is only retained as long as necessary and is securely deleted when no longer needed – ranks as the biggest compliance challenge and has done in every quarter since Q2 of 2021.

The application of the GDPR has presented some challenges. Small and medium-sized enterprises (SMEs) tend to struggle with the complex and sometimes resource-intensive requirements of the GDPR. For large corporations, especially those with cross-border operations, inconsistency in enforcement and interpretation of the GDPR by different national DPAs has been a challenge. In particular, the one-stop-shop mechanism has not worked as envisaged, and has led to cross-border cases being substantially delayed and data subjects not having a fair opportunity to participate.

Furthermore, there remain major challenges resulting from complexities surrounding cross-border data transfers. This is consistently raised as the second biggest GDPR compliance challenge, and confidence is diminishing in that area.

Finally, emerging technologies are increasingly posing new challenges in the privacy domain. The most significant change in the recent jump in DPOs identifying AI and machine learning as their organisation's biggest GDPR compliance challenge: 25% in Q3 of 2023, up 11% from last quarter. The GDPR, like many subsisting regulations, appears to not have fully envisaged the rapidity with which technologies such as generative artificial intelligence and large language models would be developed and would gain widespread societal acceptance. The GDPR was premised on a more risk-averse approach to algorithmic decision-making and to widescale data scraping to train models. But the very fast general social acceptance of the large models such as ChatGPT, DALL-E etc has confounded this approach. A few have questioned the legality of how the large models have been trained, but interestingly, the GDPR has not tended to be the basis for this, even though the training of the models is in tension with the GDPR (rather, challenges have arisen based on copyright or in jurisdictions, such as the US, where GDPR is not the focus).

Priority Issues to be Addressed:

- Simplified guidelines (with practical examples of good practice) to assist with setting and complying with retention periods. This should include guidance that intersects with AI (for example, where personal data is stored in AI prompts).
- Simplified guidelines and support mechanisms for small businesses to understand and comply with GDPR.
- Reform of the one-stop-shop.
- Clearer and more stable frameworks for international data transfers need to be developed, considering global data flows and international privacy standards.
- Very clear guidance is needed on automated decision-making by bodies exercising public functions. There is a push by some governments quickly to embed AI decision-making into public decisions, to address backlogs around, for example, social welfare decisions or immigration decisions. Guidance is needed swiftly on these matters.

2. **Exercise of data subject rights**

a. From the individuals' perspective: please provide information on the exercise of the data subject rights listed below, including on possible challenges (e.g. delays in controllers/processors reply, clarity of information, procedures for exercise of rights, restrictions on the basis of legislative measures, etc.).

Answer: I do not have access to quantitative information on this question. My answer is impressionistic based on my practice. The right of access to information remains the primary right that individuals seek to exercise. In my practice I have seen that there is increasing delay in responses by public body data controllers to access requests – rather than getting better at responding more swiftly, my impression is that the urgency that followed the implementation of the GDPR has somewhat dissipated and controllers are more likely to take longer that the permitted time limit to respond (particularly public bodies). Conversely, private body controllers are generally maintaining a high level of compliance in responding to access requests.

Awareness of other rights, particularly rectification, erasure and data portability, has increased among individuals. However, they remain less used and much less understood rights, in particular the extensive exemptions to the right of erasure.

From the controllers and processors' perspective: please provide information on the compliance with the data subject rights listed below, including on possible challenges (e.g. manifestly unfounded or excessive requests, difficulty meeting deadlines, identification of data subjects, etc.).

Answer: Again I do not have access to quantitative information on this question. My answer is impressionistic based on my practice. Controllers and processors have become much more aware of the full array of data subject rights. Both public body and private body controllers have worked hard to put systems in place to allow for the exercise of these rights although, as mentioned, my experience is that public bodies can struggle to respond within the mandatory timeframe. There has also, especially in the UK, been push-back against the use of subject access as a perceived tool of disclosure or discovery to gather employee data or as an investigative tool. It is not clear whether the recent CJEU decision on the right of access (which, I believe, takes the correct approach) will be followed in the UK, where the Courts have already suggested that the right of access can only properly be used to vindicate privacy concerns.

b. Do you avail of / are you aware of tools or user-friendly procedures to facilitate the exercise of data subject rights?

Answer: I am aware of the following tools, some of which are used by my clients:

- Data Subject Access Request (DSAR) platforms/software used to automate the management of data subject requests. Examples: OneTrust, TrustArc.
- Data mapping and inventory tools used to Identify where personal data resides in systems making it easier to locate and act upon it when a data subject exercises their

rights. Examples: Spirion, BigID.

- Consent Management Platforms (CMPs) used to manage user consents for data processing. Example: Quantcast Choice.
- Privacy Impact Assessment (PIA) software used to evaluate privacy risks associated with data processing activities.
- De-Identification and Data Masking tools used to protect personal data when sharing by removing identifiable details.
- Automated Redaction software used by organizations to quickly find and redact personal data, ensuring compliance with data subject requests.
- Chatbots and virtual assistants used to guide data subjects in submitting requests on privacy web pages
- API-based Integration tools used to Integrate with various systems via APIs to retrieve, modify, or delete personal data as needed

c. Do you have experience in contacting representatives of controllers or processors not established in the EU?

Answer: No. However, I am aware that, among the proposed UK amendments to data protection law via the Data Protection and Digital Information Bill is the removal of the requirement to appoint a UK Representative. The majority of DPO respondents to the June 2023 UK Data Protection Index Report (57%) were not at all confident in this proposed reform.

d. Are there any particular challenges in relation to the exercise of data subject rights by children?

Answer: The following are challenges that have been identified regarding exercise of subject rights by children:

- Children may not fully understand their rights regarding personal data, making it difficult to exercise their rights, although good steps have been taken to provide explanatory material in child-friendly language.
- Depending on their age and education, children may lack the digital literacy skills to navigate online platforms and exercise their rights effectively.
- Children's vulnerability may expose them to undue influence or pressure from adults, potentially affecting the authenticity of their consent or data rights exercises.
- Navigating the balance between a child's data rights and the rights of parents or guardians can be difficult. This includes determining when a child is capable of making decisions about their data independently from their parents.
- Difficulties with online age verification makes it challenging to ensure age-appropriate access without excessive data collection from children.
- Ensuring genuine parental consent and verifying the identity of the consenting

adult can be challenging, particularly online. This makes it difficult to comply with GDPR provisions mandating parental consent for processing children's data in certain scenarios.

- In educational settings, where children's data is often processed, the roles of schools, parents, and third-party service providers in respecting children's data rights can be particularly complex to navigate.

3. **Application of the GDPR to SMEs**

a. What are the lessons learned from the application of the GDPR to SMEs?

Answer: There are a number of lessons which can be learned:

- Despite initial challenges, GDPR has pushed many SMEs to adopt better data practices, leading to increased trust from clients and customers.

- Positively, SMEs often have a more flexible infrastructure and processes compared to large corporations, making some aspects of GDPR adaptation quicker and easier.

- Digital tools and software solutions facilitating GDPR compliance have been beneficial for SMEs, streamlining processes and supporting them to comply usually at affordable cost.

- SMEs benefit from straightforward, practical guidance on GDPR. Simplified instructions and templates have proven valuable. Continuous training and education are crucial in ensuring that all staff members understand and uphold data protection principles.

b. Have the guidance and tools provided by data protection authorities and the EDPB in recent years assisted SMEs in their application of the GDPR (see also the EDPB data protection guide for small business?

Answer: In my experience, and in the experience of my clients who provide external DPO functions, sometimes for SMEs, the guidance and tools provided by DPAs and EDPB in recent years have been instrumental in assisting SMEs with GDPR compliance in the following ways:

- Resources such as the EDPB's guide for small businesses have clarified GDPR requirements, making the regulation more accessible for SMEs. Guidance documents have helped SMEs to identify and prioritise the data protection risks they face. Sector-specific guidance has been helpful in addressing unique challenges faced by SMEs in different industries. The guidelines provided by DPAs and the EDPB have given SMEs the language and references required to communicate compliance measures to relevant stakeholders, including clients and regulators.

- SMEs often lack dedicated legal / compliance teams. Relevant guidance provided by DPAs and the EDPB bridge this gap by providing expertise in a simplified format. In particular, by leveraging free resources provided by DPAs and the EDPB, SMEs have been able to reduce the financial burden of seeking external DPO consultancy services. Simplified tools including checklists, templates, and FAQs have helped SMEs to implement GDPR principles in a practical, understandable manner.

- Regular updates from DPAs and the EDPB have helped SMEs keep abreast of new developments and changes in data protection laws and practices which affect their business.

c. What additional tools would be helpful to assist SMEs in their application of the GDPR?

Answer:

- User-friendly interactive online platforms that guide SMEs through a tailored compliance process, considering their specific industry and size.

- A broader range of customizable policy and procedure templates, including data protection impact assessments, processing records, and breach notification protocols.

- Simplified guidance on how to integrate GDPR compliance into common SME tools and software, such as CRM systems and e-mail marketing platforms.

- A collection of anonymized/fictional compliance and breach case studies from which SMEs can learn, illustrating practical examples of challenges and solutions. Data breach simulation tools to help SMEs conduct mock data breach exercises, helping them prepare and respond effectively to actual breaches.

- Easy-to-use risk assessment software that helps SMEs identify and manage data protection risks associated with their specific business activities without having to incur huge cost of undertaking those costs through consultants.

- Dedicated helpline or an AI-driven chatbot service for SMEs to get quick, reliable answers to GDPR-related queries

4. Use of **representative actions** under Article 80 GDPR

a. Would you like to give feedback about any representative actions in any Member State?

Answer: There is some academic analysis which suggests that Article 80 has not been implemented consistently, or satisfactorily, across the EU. See Pato, Alexia, "The Collective Private Enforcement of Data Protection Rights in the EU" (2019). Available at https://dx.doi.org/10.2139/ssrn.3303228. The use of representative actions will

further be discouraged in those Member States who have chosen not to allow representative bodies on an "opt-out" basis, as even if a representative body passed the test set in Article 80(1), it would still have the large and time-consuming task of having to collect signatories to the claim. On 23 February 2021, the UK Government set out its reasons for declining to enact Article 80(2), despite most children's rights groups and privacy organisations being in favour of doing so.

5. **Experience with Data Protection Authorities (DPAs)**

a. What is your experience in obtaining advice from DPAs?

Answer: Generally positive, although the advice has not tended to be particularly in-depth and is often non-committal. It appears that the main reason for seeking advice from a DPA is in order to demonstrate accountability and to tick the box of having asked the regulator (a mitigating factor, if needed), rather than in the hope of a clear substantive steer.

b. How are the guidelines adopted so far by the EDPB supporting the practical application of the GDPR?

Answer: In my experience, my clients find the EDPB's guidelines very helpful:

- Specifically, my clients who operate as external DPOs (in both UK and EU) find the guidelines play a key role in supporting the practical application of the GDPR by providing clarity, consistency, and practical advice on various aspects of the regulation. My clients felt that the EDPB guidelines help to translate legal requirements into operational steps that organizations can implement, bridging the gap between legal theory and practical application. The guidelines on data breach notifications were singled out as helpful, as were sector-specific guidelines and the guidelines on international transfers.

- My clients emphasised that valued the harmonising role played by EDPB guidance, reducing the risk of divergent interpretations and practices among Member States

- My clients also valued that, as new technologies emerge, the EDPB seeks to issue guidelines to address how the GDPR applies to these technologies, for example the 17 May 2023 Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement.

c. Are DPAs following up on each complaint submitted and providing information on the progress of the case?

Answer: No. The issue has been the subject of very recent litigation in the UK, in the case of *R(Ben Peter Delo) v The Information Commissioner* [2023] EWCA Civ 1141, which ruled on the meaning of Article 77 of the UK GDPR (the wording of which is the same as Article 77 of the GDPR). The Court of Appeal held that the Information Commissioner was not obliged to determine the merits of each and every complaint,

but instead had a discretion to decide another appropriate outcome, having first investigated the subject-matter to the extent appropriate. The Court of Appeal further held that an 'outcome' must be the end of the Information Commissioner's 'handling' of a complaint. A conclusive determination or ruling on the merits that brings an end to the complaint is an 'outcome', but so is a decision to cease handling a specific complaint whilst using it to inform and assist a wider industry investigation. It was also open to the Information Commissioner, on a complaint that a subject access request had not been handled properly, to review relevant correspondence and advise the data subject that it was likely that the controller had complied with its obligations, making clear that no further action would be taken .

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

Answer: Yes. The UK ICO guidance is detailed and generally well-received, and remains helpful for those in the EU given the extent to which there remains significant overlap between the GDPR and the UK GDPR. There has, however, been some divergence. For example, the ECPB and the ICO have taken different approaches in guidance and recommended tools for conducting Transfer Impact Assessments (TIAs) or Transfer Risk Assessments (TRAs). The ICO's TRA tool for conducting TIAs is relatively light touch, focussing on whether the circumstances of the data transfer significantly increase the risk to the privacy and other human rights of the individuals and whether the transfer mechanism will be enforceable against the third country importer. This contrasts with the EDPB approach which requires organisations to conduct an in-depth examination of the legal environment to which personal data will be sent. In addition, the ICO's TRA tool allows organisations to proceed with carrying out what it refers to as low harm risk transfers without needing to conduct any local law assessment at all unlike the EDPB approach, which requires local law assessment to be conducted in all scenarios and only allows organisations to take the circumstances of a proposed transfer into account when identifying effective supplementary measures to protect the data being transferred. On the other hand, there has been convergence between the ECPB and the ICO on guidance on issuing penalty notices and calculating fines.

6. Experience with **accountability** and the **risk-based approach**

a. What is your experience with the implementation of the principle of accountability?

Answer: Generally, the accountability obligations under the GDPR have driven a more active and documented approach to data protection, which can be a significant shift for some organisations. While there are often complaints about the challenge of keeping the requisite records, it is notable that research is starting to be published about the significant business benefits of accountability and the implementation of data privacy management programmes, including giving a competitive edge by boosting trust; promoting operational efficiency; making the organisation more attractive to investors, encouraging greater agility and innovation, leading to demonstrable and significant cost benefits: see the CIPL and Cisco January 2023 Report.

b. What is your experience with the scalability of obligations (e.g., appropriate technical and organisational measures to ensure the security of processing, Data Protection Impact Assessment for high risks, etc.)?

Answer: Global companies tend to have policies across the board, but the implementation is not always uniform across teams. Generally, my DPO clients see that the bigger the company/organisation, the more they seem to find it difficult to enforce and implement their obligations. So one tends to find more inconsistencies across bigger companies in terms of their data compliance than with smaller businesses.

7. **Data protection officers** (DPOs)

a. What is your experience in dealing with DPOs?

Answer: My clients who support internal DPOs say that:

- Internal DPOs are most concerned about:
  - Lack of independence. They often have to wear multiple hats in their organisations and do not feel they can act with sufficient autonomy.
  - Lack of resources. DPOs typically require the support of a team, in particular in large and complex organisations. They typically have to cover an extensive area of responsibility with little or limited resources and state that this can lead to non-compliance.
  - Lack of senior buy-in or support. In some organisations the lack of senior support can result in the DPO feeling very frustrated in their efforts to mature the data protection and privacy programme in a business.
- Internal DPOs are most positive about:
  - The opportunity to influence the strategy and direction of a business at the most senior levels.
  - Continuously evolving landscape and an opportunity to mitigate the risk of emerging technologies whilst capitalizing on the opportunities.
  - Working with all the different parts of an organisation and an opportunity to collaborate on key matters impacting all functions and individuals – be they employees, customers or shareholders.

b. Are there enough skilled individuals to recruit as DPOs?

Answer: Yes, although there is a general growing demand for quality DPOs.

c. Are DPOs provided with sufficient resources to carry out their tasks efficiently?

Answer: There is a mixed picture, with some organisations providing ample support while others struggle to meet the necessary standards:

- Large Corporations and Tech Companies: Many large corporations, especially in the technology sector, tend to allocate substantial resources to their DPOs. These organisations often face significant data protection challenges due to the scale of their data processing activities and the sensitivity of the data they handle.

- Public Sector Organisations: In the EU, public sector organisations, due to their obligation to comply with GDPR, often provide their DPOs with adequate resources. This is particularly true for public health organizations, government agencies, and educational institutions that process large amounts of personal data.

- Small and Medium-sized Enterprises: SMEs can struggle with resource allocation for DPO roles.

- Industry-Specific Cases: In industries where data is a critical asset, such as finance, healthcare, and e-commerce, there tends to be a higher level of resource allocation for DPOs. For example, major banks and healthcare providers often have well-resourced data protection teams to handle the sensitive nature of the data they process.

- Startups and Tech Innovators: The situation in startups can vary widely. Some prioritise data protection from the outset and allocate resources accordingly, while others may overlook or under-resource this area in the early stages of development.

- Non-profit Organisations: Non-profits and NGOs often face resource constraints and may not be able to provide their DPOs with sufficient resources, which can impact their ability to comply with data protection regulations effectively.

d. Are there any issues affecting the ability of DPOs to carry out their tasks in an independent manner (e.g., additional responsibilities, insufficient seniority, etc.)?

Answer: Yes. They include:

- Additional responsibilities within the organisation that conflict with their duties as a DPO, which can compromise their independence.

- Insufficient seniority and lack of direct line of communication to the highest level of management, which may hinder the authority / influence of the DPO to effect necessary changes or have their recommendations taken seriously.

- Lack of sufficient support from senior management, which may cause the DPO to struggle to enforce data protection measures, especially if these measures are seen as an impediment to business goals or operational efficiency.

- Evaluating DPOs based on metrics that are incompatible with their data protection responsibilities, such as contributing to revenue targets can create a conflict of interest and pressure the DPO to compromise on compliance issues.

- A lack of protection against retaliation for performing their duties can compromise a DPO's independence. DPOs should be able to advise and act without fear of repercussions for their employment status or career progression.

- A corporate culture that does not value or understand the importance of data protection can hinder the DPO's ability to carry out their role independently. If the organisation sees GDPR compliance as a checkbox exercise rather than an integral part of operations, the DPO may not be able to effectively advocate for necessary changes or resources.

- Insufficient resources can limit their ability to stay informed, provide training, and perform their tasks effectively.

8. **Controller/processor relationship (Standard Contractual Clauses)**

   a. Have you made use of Standard Contractual Clauses adopted by the Commission on controller/processor relationship (Commission Implementing Decision (EU) 2021/915.)?

      Answer: Yes

   b. If yes, please provide feedback on the Standard Contractual Clauses?

      Answer: In general, SCCs serve a great functional purpose, and the move to the new SCCs plus modules plus the UK Addendum has been relatively straightforward. However, SCCs can at times be difficult to implement. While they are quite effective at securing private sector entities applying an equivalent level of protection for personal data, they are not well placed to precent third country public authorities from accessing personal data. Module 4 has also caused confusion as to when it would ever be appropriate for a processor (vendor) to impose contractual terms on a controller (customer). Module 4 is the least workable. Furthermore, in most/ all instances, a non-EU controller importer will be themselves required to comply directly with the GDPR under Article 3(2) so that the EU SCCs are not available anyway (as confirmed in recital 7 of the Commission Implementing Decision EU 2021/914).

9. **International transfers**

   a. For <u>controllers and processors</u>: Are you making use of the Standard Contractual Clauses for international transfers adopted by the Commission (Commission Implementing Decision (EU) 2021/914)? If yes, what is your experience with using these Clauses?

   b. For <u>controllers and processors</u>: Are you using other tools for international data

transfers (e.g., Binding Corporate Rules, tailor-made contractual clauses, derogations)? If yes, what is your experience with using these tools?

Answer: My clients have experience using BCRs. One point which has been highlighted to me is that BCRs mean regular (certainly during the initial approval process) and very close contact with EU regulators. It is well known that the approval process can be overly lengthy, depending on the BCR Lead's country of establishment. Companies seeking BCRs need to have a certain level of privacy compliance maturity, given that at least initially, they will be under quite intense regulatory scrutiny. The big advantage is that once the approval process is over, BCR companies are generally more trusted by the regulators and transfers subject to BCRs tend to be less scrutinised.

c. Are there any countries, regional organisations, etc. with which the Commission should work in your view to facilitate safe data flows?

Answer: Yes. **Africa** – As African countries continue to develop their digital economies, there is a growing need for collaboration to ensure that any data flows to and from the EU meet GDPR standards. Particular focus should be given to countries regularly receiving / making significant tourism and business visits from / to the EU such as Kenya, South Africa, Rwanda, Ghana, and Nigeria.

10. 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.)?

Answer: While the UK GDPR closely aligns with the EU GDPR, there are some divergences in certain provisions. These differences may require organisations to implement additional measures or modify existing processes to meet the requirements of both regulations.

11. **Fragmentation/use of specification clauses**

a. Please provide your views on the level of fragmentation in the application of the GDPR in the Member States (due to Member State implementation of the GDPR or the use of facultative specification clauses, such as Articles 8(1) and 9(4) GDPR).

Answer: Implementation and enforcement of the GDPR at the national level have introduced a level of fragmentation in the regulation's application. The facultative specification clauses have allowed member states to make their own interpretations, leading to discrepancies in enforcement and application. This variability creates challenges for organisations operating across multiple EU countries, as they may need to adjust their policies and practices to comply with each country's interpretation of the GDPR.

Despite significant efforts by the EDPB and national DPAs to reduce inconsistencies, some degree of fragmentation will likely persist. This is due to the perpetual tension

between the desire for a unified EU-wide approach and the sovereignty of member states over certain aspects of their legal systems. Overall, the dialogue between member states, institutions, businesses, and the EDPB is crucial in identifying and addressing this fragmentation to ensure that the GDPR remains effective.

b. Please specifically identify the area in which you consider there to be fragmentation and whether it is justified.

Answer: Article 8(1) GDPR allows member states to legislate different ages at which children can consent to data processing in the context of information society services, within a range of 13 to 16 years. This has resulted in a lack of uniformity across the EU, complicating the design of services targeted at children. While it may initially have seemed a sensible compromise, this divergence is increasingly anachronistic, particularly given the evidence of harms across these age ranges from online platforms.

There are other areas of fragmentation, but where that appears still to be justified, despite the additional burdens it imposes:

- Article 9(4), which enables member states to introduce further conditions, including limitations, regarding the processing of genetic data, biometric data, or data concerning health). This has led to a patchwork of different standards and regulations across the EU that organizations must navigate.
- Article 36(5), which requires controllers to consult or obtain authorisation from the DPA for processing for a task in the public interest.
- Article 49(5), which permits national laws to limit transfers of specific categories of personal data.
- Article 80(2), which allows national governments to authorise privacy organisations to lodge complaints and institute court actions independently from a mandate by data subjects.
- Article 89(2) and (3), which allow national law to provide for derogations from specified data subject rights in so far as such rights are likely to render impossible or seriously impair the achievement of specific purposes.

12. **Codes of conduct, including as a tool for international transfers**

a. Do you consider that adequate use is made of codes of conduct?

b. Have you encountered challenges in the development of codes of conduct, or in their approval process?

Answer: Although I am aware that a number of national codes of conduct have been adopted across Europe, and of the transnational Data Protection Code of Conduct for Cloud Infrastructure Service Providers (Feb 2021) and EU Cloud CoC (June 2021) – the latter perhaps being the most successful code of conduct – I do not think that adequate use is made of codes of conduct, or that they have lived up to the intention of the GDPR.

In early 2020, the UK ICO formally invited organisations to submit their sector-specific and scheme criteria for its approval, publishing guidance on developing codes of conduct and declaring that it was "open for business" on codes of conduct and certification schemes. The fact that there are still no approved UK codes of conduct, despite this supportive approach and encouragement, shows that it has proved much more difficult to develop codes of conduct than was perhaps anticipated. Challenges include:

- Determining and agreeing the exact meanings of GDPR terms and their application to specific sectors;
- Adapting the code to the specificities of national markets and laws, and considering the nature of existing processing entities;
- Ensuring broad consultations with various stakeholder groups; and
- Agreeing any broader ethical, legal or social matters which need to be taken into account and reflected in the Code of Conduct (which, for example, inform concepts like informed consent or confidentiality or data management).

c. What supports would assist you in developing codes of conduct? *Please clearly distinguish in your reply when Codes are used for international transfers.*

Answer: There are two changes I think would assist for all types of code of conduct:

- Transparency in Progress of Codes' Approvals: Competent supervisory authorities and the EDPB should publish periodic updates regarding the status of codes submitted and reasons for any delays. More transparency in the process would serve as a spur, as well as flag for others where difficulties may be encountered so that they can take pre-emptive action for any codes of conduct they may be promoting.

- Specificity in Review/Approval Timelines: Linked to the first suggestion, clear timelines should be set for competent supervisory authorities to finish their review and approval. Supervisory authorities could adopt their own timelines, or the EDPB guidelines could specify the duration allowed (both for national codes and for any transnational codes submitted to the EDPB. Differentiation in timelines could reflect that some types of code would be expected to take a shorter period than others for review/approval.

13. **Certification, including as a tool for international transfers**

a. Do you consider that adequate use is made of certifications?

Answer: Adequate use has not been made of certifications, partly because the development of Article 42 and 43 schemes has been slower than expected. There has also been a certain amount of confusion around whether the European Data Protection Seal can be used for processes related to international transfers. Some advisors take the view the answer is a strict 'no', others say yes, if combined with other binding and enforceable commitments. The ECPB's Opinion 28/2022 has not laid that debate to rest.

b. Have you encountered challenges in the development of certification criteria, or in their approval process?

c. What supports would assist you in developing certification criteria?

Answer: I have not been involved in the development of certification criteria, or in their approval process.

14. **GDPR and innovation / new technologies**

a. What is the overall impact of the GDPR on the approach to innovation and to new technologies?

Answer: The GDPR has allowed for development of AI and newer technologies with at least some thought given to data protection. The use of innovation sandboxes has been helpful in promoting data protection compliant innovation. However, it appears to me that the vast majority of recent leaps forward in generative AI have been achieved with only peremptory thought being given to the protection of personal data and to ensuring there are robust legal bases for the processing of personal data in datasets used to train the models.

My fear is that one of the reasons that the GDPR has not been seen as a hinderance to the development and application of AI to personal data is that the true extent of how personal data has been scraped and used, and of how much new embedded automated decision-making is taking place, is not widely understood (this is itself a challenge to the GDPR).

Going forward, there is plainly going to need to be guidance on various aspects of AI. I have already flagged that simplified guidelines (with practical examples of good practice) are needed, for example on retention periods, including for training data and personal data is stored in AI prompts. Examination is also needed of the extent to which AI providers and AI users are joint controllers, given that many current AI users are influencing the training of the AI, particularly in terms of conversational capabilities.

A key area of concern is the push by some governments quickly to embed AI decision-making into public decisions, to address backlogs around social welfare decisions or immigration decisions. Guidance is needed swiftly on these matters.

b. Please provide your views on the interaction between the GDPR and new initiatives under the Data Strategy (e.g., Data Act, Data Governance Act, European Health Data Space etc.)

Answer: In general, the aim of the Data Strategy, in particular in extending good data governance into the IoT and B2B contexts, and to non-personal data, is to be applauded. Facilitation of sharing of protected data is also welcome. It is very early days, but the initial interaction between the GDPR and the new initiatives has been tricky, for a number of reasons:

- The terms of the GDPR and the Data Act are not aligned, and the Data Act introduces a number of new terms, such as "data holder" and “users”, whether they are data subjects or not. Applying these new terms to GDPR terms is not straightforward. The Data Act offers limited guidance, and roles must be evaluated on a case-by-case basis, considering who effectively determines the purposes and means of processing. Given the ambiguity in this area and lack of regulatory guidance, it is probable that data holders and users will need to define their roles based on general GDPR principles.

- The Data Act also requires designers of connected products to implement good data management practices. Article 3 states that connected products shall be designed and manufactured so that the data are easily accessible, secure, machine-readable and if possible, directly accessible to the user by default. The same applies to the related service data including meta data. This takes the GDPR provisions of data protection by design and by default one step further, as it impacts product design and documentation directly for all making connected products available to users. The goal is to make the data directly accessible to the user. While this provision is very much aligned with the European Data Strategy, data holders and manufacturers should also be careful not to provide access to unauthorised persons, as this could constitute a data breach.

- The AI Act in particular appears to be in tension with the GDPR. This will be ameliorated to some extent if the CJEU upholds the decision in *Single Resolution Board v European Data Protection Supervisor* (Case T-557/20) on pseudonymised data being considered anonymised if the holder of the data has no means to re-identify the individuals.

22 November 2023

ESTELLE DEHON KC

CORNERSTONE BARRISTERS
2-3 GRAY’S INN SQUARE
LONDON, WC1R 5JH
estelled@cornerstonebarristers.com