SHOOSMITHS

European Commission call for evidence on the Application of the General Data Protection Regulation (GDPR)

08 February 2024

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?

Benefits

- There is no doubt that the GDPR has raised the standard of protection afforded to individuals, both those located in the EU as well as outside the EU where personal data is processed by EU organisations. Indeed, the GDPR has been impactful on a worldwide basis by helping to set a new global standard of data protection that a number of new international data protection laws have sought to emulate. Taken together, this has instilled a greater awareness across the international community of key principles such as data subject rights, accountability and transparency.
- The GDPR has prompted organisations to map the use, location and movement of personal data yielding commercial and organisational benefits and assisting with compliance governance in other areas, whether sector-specific or future areas (e.g. the proliferation of AI-power services). It has also led to a marked improvement in the level of diligence of the treatment of personal data within supply chains and the application of more robust contractual and organisational controls. Mandatory risk assessments have allowed for more faithful implementation of the data protection principles enshrined in Article 5 GDPR.
- The rights conferred by the GDPR on individuals has led to better transparency in respect of the use of personal data and the identity of the organisations using it. It has also empowered individuals to demand better engagement when exercising their data protection rights, both those that existed under the Data Protection Directive (and were enhanced by the GDPR), as well as the new rights introduced by the GDPR.

Challenges

- The regulatory burden in relation to routine and low risk processing is still too high, despite the risk-based approach accommodated in many areas of the GDPR.

- The regulatory burden for SMEs is also too high and in many cases the GDPR takes a 'one size fits all' approach which is unrealistic and ultimately not an enabler for better compliance.

- Divergence among Data Protection Authorities' ("**DPA**s") approaches in managing infringements of the GDPR with varying application of enforcement action has led to inconsistency.

- Inconsistency in the interpretation by DPAs, by way of example only, to the use of cookies and the concepts of personal data and anonymisation, has undermined the creation of a harmonised standard and the certainty required by organisations to discharge their compliance obligations effectively.

- The primacy of consent over other lawful bases in certain areas, especially in conjunction with the ePrivacy Directive, poses significant challenges for organisations. This is particularly evident in the adtech and automotive sectors where the need for consent can

unduly restrict benign use cases. We suggest the Commission explores avenues to allow multiple options of lawful bases to coexist without consent overriding legitimate interests unnecessarily and consider establishing clearer guidelines or a whitelist of processing activities that can help harmonise interpretations and applications

2. **Exercise of data subject rights**

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.).

- As we primarily represent controllers and not individuals our insights are predominantly drawn from our experience in advising our clients. In that regard, we observe that individuals have become more aware of their data protection rights, in particular their rights to access a copy of their data and have their data erased. Many organisations have experienced the use of those rights to apply commercial pressure in disputes and arguably to support use cases that are unduly burdensome for organisations.

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.).

- Increased guidance on controllers managing and responding to vexatious, manifestly unfounded or excessive requests would be welcome, as well as situations where numerous requests are received in high volumes (for example, some organisations have reported receiving 25,000 requests in a day). In particular, given the emergence of companies that provide services allowing organisations to be contacted on an individual's behalf, where that individual may have had limited to zero contact with that organisation, these rights have created an administrative burden for the organisations acting as controllers, and in many cases, the processors they instruct.

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

- We are aware of commercial request tools, as well as portals provided by regulators that allow for the submission of data subject rights requests. Whilst these tools do not typically expedite administrative steps (such as identify verification), they do provide a degree of formality and standardisation that can be helpful to controllers and individuals alike.

- There are certain industry-led initiatives which have had some success in allowing data subjects an easy mechanism to exercise their rights across multiple controllers, for example the DAA opt-out mechanism. However, we believe that further initiatives in this space would have a privacy-enhancing effect.

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

- No, but we do regularly act for clients who are organisations with establishments outside the EU only and whose processing activities would give rise to the requirement for an Article 27 GDPR representative (EU Representative).

- We find that the EU Representative mechanism is not well understood by non-EU organisations and greater advocacy and enforcement action to secure compliance here will go towards improving the propensity for non-EU organisations to adhere to the GDPR's principles.

- On the other hand, we have also encountered experiences where both regulators and privacy advocate groups have misinterpreted the Article 3 GDPR test for

GDPR applicability, resulting in instances where controllers not subject to the EU GDPR have received compliance requests from EU DPAs. Clarification regarding the potential concurrent applicability of Article 3(1) and 3(2) would also be welcome by the EDPB and DPAs.

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

  Yes. We have seen the following issues relating to data subject access requests (DSAR) relating to children and which the black letter of the GDPR is ill-equipped to address:

  1. parents typically make requests on behalf of their children, and the disclosure of such information to the parent may relate to a safeguarding issue which is caused by the parent. This scenario typically plays out in a childcare setting, where a child complains to a teacher of potential abuse issues, social services are then involved, and the parent issues a DSAR to find out what the child complained about;
  2. as parents make requests for data, it may be challenging to determine whether the individual making the request has the correct legal authority to make such a request. In a typical request scenario, where a person makes a DSAR on behalf of another individual, a letter of authority can be provided. In the context of a child, letters of authority are not required, and so it is difficult to determine if a person is indeed a parent or authorised carer for a child without seeing a birth certificate or other official documentation; and
  3. in a childcare context, where a parent is in a dispute with a childcare provider, they may request data on behalf of all of their children (which may relate to a number of people) and themselves to apply pressure in connection with a related matter. The parent effectively is able to make multiple requests with one request.

  The above examples are illustrative of this being an area where greater harmonisation is needed, not just in respect of divergent approaches across DPAs, but also where the GDPR interplays with other legislation, such as the DMA/DSA.

  In light of the Commission's legislative initiatives to further safeguard children in the digital sphere, organisations would welcome specific processing conditions relating to both the processing of children's data and the exercise of their rights.

  In this regard, we would point the Commission to the UK approach (established whilst the UK was an EU Member State) where, pursuant to the UK Data Protection Act 2018, there already exists an extensive list of derogations/processing conditions to special category data processing, with specific provisions relating to safeguarding children.

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

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

   - Specific guidance and awareness raising by DPAs has been key to better compliance outcomes. The GDPR is too indigestible without that support and the translation of the requirements so that they can be understood and operationalised by an organisation with limits on its time, resources and budgets has helped to improve engagement by the SME community. However, overall, we believe there is still work to be done to improve the level of compliance amongst SMEs.

   - The review of the GDPR presents an opportunity to better balance privacy protection with the operational realities of SMEs. The current exemption under Article 30(5) does not significantly reduce the compliance burden, as SMEs still need to document their data processing activities comprehensively. We advocate for clearer guidance on balancing principle-based obligations with practical compliance requirements, reducing the undue burden on SMEs.

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)?

- In some cases DPA guidance has contributed positively to assisting SMEs, such as GDPR-readiness checklists and simply DPIA tools. However, as per our previous response, inconsistent guidance across DPAs and a lack of a harmonised approach has also created complexity to a degree that it unduly burdensome for SMEs. The most useful and digestible material has been published by small consultancies and private press.

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

- Some of our clients that are SMEs have struggled with the requirement to appoint a DPO and there is increasing debate as to whether SMEs of a certain size and turnover should be exempt from such a requirement.

- Assistance with the proportionality and extent of the DSAR obligations would also assist SMEs which are consumer-facing organisations.

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

a. From the controllers and processors' perspective: are you aware of representative actions being filed against your organisation(s)?

No.

b. For civil society organisations: have you filed representative actions in any Member State (please specify: complaint to DPA or to court, claim for compensation; and the type of GDPR infringement) and if yes, what was your experience? Do you intend to take actions under the Representative Actions Directive?

The GDPR's enforcement has been inconsistent, with a notable lack of significant case law despite being in force for nearly six years. NGOs and representative bodies have played a crucial role in addressing complex issues and bringing mass complaints, acting as a vital complement to regulatory enforcement. Their actions, while sometimes seen as challenging by DPAs, have a substantial deterrent effect on organisations, emphasising the need for regulatory support and endorsement of their privacy-enhancing efforts.

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

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

- The quality of advice from DPA websites varies. Assistance obtained through various helplines (or similar) operated by DPAs tends to address only very basic queries and access to guidance and expertise for more complex matters is often limited.

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

- The EDPB guidelines are not generally focussed on practical applications but more on clarification of the law. Where they are intended to support operational privacy e.g. guidance on supplementary measures, they are too far removed from the commercial realities of privacy governance.

- Example scenarios in EDPB guidelines often cover obvious applications of the law and so forgo the opportunity to cater for more complex circumstances.

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

- Our experience here has been mixed. In certain cases we find DPAs actively follow-up on complaints to the point of resolution, but have observed that some DPAs take a more priorities-based approach to complaint handling and, in some cases, will not engage further once an initial filing has been submitted.

- We would advocate for the Commission/EDPB enhances their respective monitoring roles to ensure complaint handling is both effective and consistent across DPAs, whilst having due regard for the disparity in resources available across DPAs.

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

- We are acutely aware of divergent guidance and interpretations taken by DPAs which, in certain cases, concern material points of the GDPR and ePrivacy Directive. Examples include differing approaches taken to consent requirements for compliant cookie banners and the interpretation of "monitoring" within the meaning of Article 3(2). There has also been significant divergence in relation to the extent to which transfer impact assessments must be performed at certain levels of the supply chain.

6. Experience with accountability and the risk-based approach

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

- Most of our clients have established processes in place to ensure they are compliant with the principle of accountability; namely internal DPIA templates that are cascaded across business functions and form a key part of any internal approval process.

- In addition, a number of clients have obtained automated software in order to ensure compliance with the accountability principle and through which ROPAs and data mapping templates are regularly updated.

- We do note, however, that recent regulatory scrutiny around the GDPR's international transfer framework has introduced uncertainty within many organisations as to whether a risk-based approach is even permissible under the GDPR. As mentioned above, the significant divergence in different regulatory guidance in relation to the extent to which transfer impact assessments must be performed at certain levels of the supply chain has been unhelpful and left organisations unclear as to the extent of their obligations.

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.)?

- Due to the generality of terms such as appropriate technical and organisational measures and the broad interpretation in how these principles are adhered to, sector based guidance would be helpful to ensure that organisations are investing in the right security products and technology to safeguard the personal data collected, in relation to the sector in which they are operating.

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

a. What is your experience in dealing with DPOs?

- Varied. Those operating at group level for large organisations tend to be experienced and capable. We note that many DPO roles are still held by those 'double hatting' with legal adviser or board roles which brings into question whether they have the requisite independence to perform the role. Many smaller businesses have junior DPOs but the processing activities and complexity of privacy issues does mean they are often ill-equipped to deal with these without external advice.

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

- Certainly not when the GDPR came into force, but the talent pool has developed, as has support and training, and there does appear to be a greater degree of supply today. In EU Member States where DPOs were already established pre-GDPR e.g. Germany, there have been fewer issues with the availability of skilled DPOs.

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

- This varies by industry but generally many data protection and privacy functions are under-resourced.

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.)?

- See reply to (a) above.

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

a. Have you made use of Standard Contractual Clauses adopted by the Commission on controller/processor relationship?

- No. We have not seen any meaningful take up of these clauses as most organisations prefer to adopt clauses with bias so that they incorporate variations of the clauses favourable to them

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

9. **International transfers**

a. For controllers and processors: Are you making use of the Standard Contractual Clauses for international transfers adopted by the Commission? If yes, what is your experience with using these Clauses?

- Yes, and our clients do so too. The Standard Contractual Clauses are helpful as they provide a streamlined, standard and widely accepted transfer mechanism to satisfy the applicable requirements of Chapter V of the GDPR. However, we do have the following feedback having advised many clients in respect of the Standard Contractual Clauses:

- The 2021 Standard Contractual Clauses do not cater for transfer from a processor to a controller that is not the processor's controller which means they are not as flexible as the UK IDTA.

- We note the current 2021 Standard Contractual Clauses are not suitable for importers whose processing operations are subject to the GDPR pursuant to Article 3, as they would duplicate and, in part, deviate from the obligations that already follow directly from the GDPR. We further note from the Commission's FAQs on these Standard Contractual Clauses that the Commission is in the process of developing an additional set of Standard Contractual Clauses that could be used in such a scenario where the importer is subject to the GDPR under Article 3, and these additional Standard Contractual Clauses will take into account the requirements that already apply directly to those controllers and processors under the GDPR. However, in the interim, it would be very helpful if the Commission could provide clarification as to what would constitute an appropriate mechanism under Article 44 GDPR where the importer is subject to the GDPR directly under Article 3. At present, it is unclear how controllers and processors operating in such a scenario can comply with the requirements of Chapter V GDPR in circumstances where there is a desire to rely on Standard Contractual Clauses (which are the most commonly utilised transfer mechanism).

- The extent to which liability may be limited under the Standard Contractual Clauses is a point which is often debated in contract negotiations. We note the Standard Contractual Clauses expressly provide that "each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses". It is not clear whether or not limiting liability would contradict this provision. It would be helpful if the Commission could provide guidance setting out the concrete position and clarifying this issue, this will reduce lengthy back and forth negotiations that occur in respect of this topic.

- It would also be helpful if adopting a risk-based approach to transfer impact assessments in a similar manner to the UK Information Commissioner's Office could be considered, in particular, to assist smaller and medium sized enterprises (SMEs) who do not have the same level of resources as large multinationals, and who often do not engage in international data transfers with the same risk profile. We have observed that the administrative and cost burden of carrying out transfer impact assessments is such that in practice, we do not see them always being completed where required. Adopting a proportionate risk-based approach to such assessments may assist with addressing this.

b. For controllers and processors: 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?

- We have made EU BCR-C and BCR-P applications on behalf of our clients and note first-hand how the approval process can be intensive and drawn out. This can be off-putting for businesses who might consider using them. This, in addition to the fact that a transfer impact assessment will still be required to be carried out in respect of each transfer occurring under the BCR, creates a significant administrative burden for businesses. Given the widespread acceptance of the Standard Contractual Clauses in commercial contracts, the advantages of having a BCR may not be sufficient to outweigh the cost and work involved in obtaining them in practice.

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

- Given the importance of certainty in respect of EU-US data transfers for organisations, ongoing commitment from the Commission to ensuring the success of the EU-US Data Privacy Framework should be a priority. Where genuine issues with the Data Privacy Framework, the associated Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities, or the EU-US Adequacy Decision are identified, these should be proactively engaged with by the Commission, and a resolution sought as required, in order to ensure the continuity of the Data Privacy Framework. In particular, the concerns raised as to the independence of the Data Protection Review Court established by the Executive Order should be examined and addressed if required.

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.)?

- The GDPR contains a large number of provisions that either permit or require Member States to derogate from or make additional rules. This means that although European data protection laws are more harmonised under the GDPR than they were under the Data Protection Directive, substantial national variations remain, for example in areas such as children's consent and the processing of special category data. This can pose difficulties for organisations with multiple establishments across Europe, who are trying to establish a streamlined approach

to compliance and can result in oversights occurring in respect of diverging requirements.

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).

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

- The GDPR's enforcement regime was ambitious at its inception but has faced challenges in achieving consistent application across Member States. The increasing size of fines has prompted organisations to more frequently challenge DPAs' decisions, highlighting the need for a more uniform enforcement approach.

- Our experience in both regulatory and organisational aspects of enforcement reveals a reluctance among regulators to tackle complex, fact-specific cases. This often leads to reduced fines or avoidance of investigations altogether, to minimize the risk of resource-intensive appeals. This situation has created disparate "enforcement islands" throughout the EU, diminishing the GDPR's deterrent effect. To address these challenges, we would invite the Commission to consider several strategies:

    1. **Harmonization of fining guidelines and procedural rules:** Establish uniform fining guidelines and procedural rules across the DPA network to reduce inconsistencies and improve enforcement and appeal success rates.

    2. **Rectification, cost-recovery, and monitoring regime:** Inspired by frameworks like NIS 2, empower DPAs to mandate compliance programs through third-party monitoring, moving beyond fines to ensure effective compliance.

    3. **Streamlined enforcement for clear-cut cases:** Adapt the framework to allow fast-tracked enforcement for straightforward violations, leveraging shared knowledge and practices among DPAs to address resource-intensive investigations.

    4. **Precedent and harmonisation:** Address the lack of harmonized case law by encouraging a unified approach to precedent-setting, akin to practices in competition matters, to ensure consistent interpretation and application of the GDPR.

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

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

- Codes of conduct are a useful way of developing sector-specific guidelines to help with compliance under the GDPR. However, lack of clarity as to the processes and requirements that interested parties must adhere to in order to gain approval for a code of conduct, and at times the somewhat combative approach to the approval process, may have dissuaded the business community from becoming significantly involved in their development.

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

- See directly above.

c. What supports would assist you in developing codes of conduct?

- We believe greater harmonisation and collaboration from key figures such as the EDPB and the Commission in this process will assist in achieving increased engagement, and as a result increased awareness, of the usefulness of codes of conduct as a tool.

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

a. Do you consider that adequate use is made of certifications? See replies to question 12.

b. Have you encountered challenges in the development of certification criteria, or in their approval process? See replies to question 12.

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

- See replies to question 12 above in respect of codes of conducts, which apply equally to this question in respect of certification.

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

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

- The ambiguity surrounding how compliance with certain requirements of the GDPR can be achieved in practice is a cause of uncertainty for businesses, particularly SMEs, who are trying to develop innovative technologies. Furthermore, the GDPR places an excessive administrative burden on businesses. For example, for a matter as simple as onboarding a new supplier, a business may have to update its RoPA, perform a Legitimate Interest Assessment, carry out a Data Protection Impact Assessment or Data Protection Impact Assessment screening tool, complete a supplier due diligence questionnaire, ensure specific contractual provisions are in place in line with Article 28 GDPR, update its privacy information, put an international transfer mechanism in place, and carry out a transfer impact assessment. This is in addition to existing accountability requirements to maintain various policies and procedures. For businesses who are not fortunate to have large legal and compliance functions and resources, this burden can be off putting and a deterrent to engaging with the new activity in question. Streamlining the steps controllers need to carry out in order to be in compliance, particularly where high risk or special category data is not involved in a particular project, would likely help support innovation as much as possible in this context.

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.)

- Guidance on the interaction between the GDPR and the Data Act in particular would be welcomed. We note the Data Act is without prejudice to the GDPR, which will apply to any personal data processed in connection with the rights and obligations set out in the Data Act. Indeed, the Data Act provides that to the extent users are also data subjects under the GDPR, the Data Act "*shall complement the rights of access by data subjects and rights to data portability under Articles 15 and 20 of the GDPR*". Data holders therefore need to assess carefully if the data they need to make accessible according to the Data Act would comprise personal data to avoid violating either the Data Act or the GDPR (e.g., by disclosing data which constitutes personal data without a valid legal basis, which is prohibited under Article 5(7) of the Data Act and Article 6 of the GDPR). The Data Act provides minimal guidance on how combined requirements of the GDPR and the Data Act can be practically fulfilled in scenarios such as this.