"One Year On"

ITI's response to the European Commission's questionnaire on the General Data Protection Regulation

3 June 2019

Last March, the European Commission's Directorate-General for Justice and Consumers launched a stakeholder consultation on the first year of application of the General Data Protection Regulation (GDPR). The Information Technology Industry Council (ITI) is pleased to contribute to this consultation. As the global voice of the tech sector, ITI represents leading companies from across the ICT industry, including hardware, software, digital services, semiconductor, network equipment and Internet companies. Our industry shares the goal of safeguarding privacy, and ITI and our member companies are working together with the European Commission and Data Protection Authorities (DPAs) around the world on key data protection and privacy issues, including the GDPR. In this context, ITI has recently released its *Policy Recommendations for a European Tech Agenda*, outlining concrete steps that the EU can take to advance a compelling European tech agenda for the 21st century, and containing several specific recommendations on future privacy policy.

ITI has analysed and aggregated the detailed responses shared by our member companies regarding their experience and compliance with the GDPR. We have organised the response on behalf of our members as follows: (1) a summary of key takeaways based on our member companies' responses; and (2) detailed feedback received from responding companies, grouped together in response to each listed question. To provide the Commission with the maximum amount of detail, while protecting the anonymity of all our respondents, we have shuffled and anonymised the member responses we received, question by question. We hope the European Commission finds this approach and compilation helpful in fully understanding the sincere efforts that our member companies have put into demonstrating their commitments to interoperable global privacy protection.

Key Takeaways

The adoption of the GDPR has proven to be a significant political achievement for the EU given the impact the regulation is having on privacy legislation around the world, and also for providing a comprehensive framework for crucial elements of privacy legislation – although some aspects of its implementation are in need of improvement:

- The GDPR has catalysed a rethinking of privacy at every level, resulting in real and meaningful changes, starting from the engineering and product design phases, including internal documentation of risk assessment and compliance efforts, and changing the conversation with customers by raising the awareness of data protection globally. Another positive impact is the strengthened motivation in the U.S. to advance federal privacy and data security legislation.

Global Headquarters
1101 K Street NW, Suite 610
Washington, D.C. 20005, USA
+1 202-737-8888

Europe Office
168 Avenue de Cortenbergh
1000 Brussels, Belgium
0032 (0)2 380 7764

info@itic.org
itic.org

- Our industry wholeheartedly welcomed the increased harmonisation and legal certainty the regulation has brought across the EU, which are key for the development and take up of competitiveness-enhancing technologies and services such as Cloud and Artificial Intelligence.

- However, the lack of a consistent approach for the time being by DPAs across Member States remains a challenge. Some Member State's national data protection rules have not been fully aligned with the GDPR; diverging national interpretations, including on the competency to investigate/decide a matter, create inconsistency and insecurity, which DPAs could reduce by acknowledgement that when investigating crossborder data processing activities, they will take into consideration the requirements and guidelines of the Lead Authority. A genuine, strong cooperation among the EU's DPAs is essential for a coherent application and enforcement of the GDPR across Europe.

- Given the uncertainty on the consistency mechanisms and the functioning of the one-stop shop, more compliance clarifications are needed on cross-border transfers.

- To realise the full potential and benefits of the GDPR, more guidance is essential for companies to implement the key practices while securing growth and innovation, such as data subject rights, personal data breach notification, and lawful basis of processing.

- The GDPR has become a very complex piece of legislation, affecting almost every business, but there is insufficient understanding from data subjects and customers. Our experience is that for SMEs inparticular, it is very hard to understand the GDPR' s requirements and apply them properly to their business operations.

Detailed Responses to the European Commission's Questions

1. General Comments

Privacy, security, and trust are central to our member companies' businesses, and they take seriously their obligation to protect and use responsibly the personal data in our care of customers, consumers, users, and employees. The GDPR has made a real and meaningful impact to the global privacy landscape and, working closely with regulators, our member companies have developed robust transparency measures, preference and consent tools for users, and tools to enable data subjects to more easily make requests. While most of our members already had high data protection standards, GDPR helped further strengthen the focus on data subjects rights and enhance harmonisation and legal certainty.

Our companies approach the GDPR as the latest step in their privacy commitment to transparency, user control, and rights of the individual. These efforts require thoughtful investment, assessment, and devotion to the readiness effort. The GDPR has truly driven a rethinking of privacy at every level and our companies have observed both benefits and challenges throughout the process.

1.1 Positive impacts that have emerged from the implementation of the GDPR

- **Privacy by Design**
  Privacy by design fits into our member companies' existing customer-centric business models. Codifying privacy by design in the GDPR has facilitated increased operational rigor around the product life cycle, which results in further maturation of privacy compliance, product life cycle processes, and user design experiences that benefit consumers and the business. In addition,

data protection impact assessments (DPIAs) also facilitate the inclusion of privacy mechanisms in the product throughout the development process and prior to processing. The GDPR is setting flexible standards around privacy by design that leads to truly innovative privacy practices by allowing creativity and tailored processes based on company and customer rights and needs.

- **Organised Data**
  The GDPR increases the existing urgency for companies to organise their data collected through consistent data taxonomies and standards across all products. Organised data is valuable to fulfil customer data subject requests. For example, if a data subject submits a data deletion request, organised data helps to identify the data associated with the data subject, and how, where, and with whom the personal data has been shared with others. Organised and consistent data also improves the ability to leverage the data efficiently, which ultimately improves product offerings and customer experience.

- **Increased Awareness**
  The GDPR has transformed the way governments, businesses, and society think of data protection, and strong and robust privacy practices are in the interests of all stakeholders. The private sector has responded to the GDPR positively by incorporating core elements into organisational design and culture, as well as innovating with a customer-centric mindset that makes stronger connection to its consumers. Another positive impact of the GDPR implementation is the strengthened motivation in the U.S. to advance federal privacy and data security legislations, and we support these efforts as we believe all individuals across the globe deserve adequate privacy protections.

1.2 overarching challenges emerging from the first year of the GDPR's implementation

- **Lack of Harmonisation Among DPAs**
  Not all Member States' domestic data protection laws have been updated, and where they have been updated, national divergences remain, especially on the age of consent to data processing. With different interpretations and positions from the DPAs, companies have to make additional investments in product development to adapt to the national differences. For example, it is difficult to determine the level of detail of the information to be provided to data subjects under articles 13 and 14 of the GDPR. This problem is exacerbated by extensive interpretations of the GDPR by DPAs and the CJEU. This not only introduces an element of unpredictability in business operations, but also most importantly prevents full harmonisation for business and for user experiences across Europe and goes against the objective of achieving a true Digital Single Market (see additional comments below.)

- **Uncertainty on One-Stop-Shop and Consistency Mechanism**
  Uncertainty remains over the functioning of the one-stop-shop and the consistency mechanism. As regulators take unilateral action on cross-border data processing issues, companies need clarity about what is permitted, and what is not permitted so that industry has guidance and clarification regarding compliance with the GDPR to the best extent possible.

- **Insufficient Guidance on Key Practices**
  The GDPR has upheld some key concepts and values that are critical to individuals on a range of important topics and rights. However, in order to realise and achieve the positive objectives of the rules, further clarity and guidance on obligations and scope are needed. Below are some key

aspects where our companies would appreciate further guidance and a balanced approach that takes into account the specific complexities of each of them:

- Data Subject Rights: While our companies strongly support enabling the exercise of data subject rights in a way that is effective, efficient, and reasonable, timely compliance with the obligations set forth in Chapter 3 of the GDPR in relation to data subject rights can present some challenges. For example, the difference in data subject rights is not always clear relative to different populations (e.g., professional/adult populations vs. vulnerable populations vs. consumer populations); deletion and access often require manual and time-intensive intervention. While there are technologies that can help make fulfilling requests easier, as of today, there is no solution that can fulfil such rights automatically, especially in large, global organizations which require a significant number of very diverse applications; additionally, the right to object to personal data processing based on legitimate interest could result in companies being unable to provide the product or service at all; furthermore, the right to access should not be used as a tool to disguise data fishing expeditions in order to gather evidence for future litigation. Companies and industry would request guidance on a balanced approach to fulfilling these rights without interrupting business operations when possible, especially interpretation of the law that allows for protection but does not have the unitended effect of raising costs for the individual, hampering innovation, or preventing access to an otherwise useful and desirable service.

- Personal Data Breach Notification: It often takes at least 7 to 30 days of investigation to ascertain how a data breach occurred and understand the extent of the breach. While the industry appreciates the risk-based approach taken in the GDPR to determine when breach notification is required, the 72-hour timeframe is too short to provide meaningful information about a breach. A breach by itself likely to result in significant reputational harm to the affected company. To make matters worse, a premature notification before grasping the whole picture, bears additional risk to the business and impacted customers. Premature notification can pose risks to users if the breach is not fully contained or if conflicting notices lead to confusion. For example, at the early stages when notification is required, companies may not know the full extent of the breach and may not be able to identify the most appropriate remedies, which would not benefit the individuals affected by the incident. We recommend that notification be required only once the full extent of the incident is understood and then as quickly as reasonably possible.

- Lawful Basis of Processing: Operationalising the application of the lawful basis of processing is sometimes signalled by companies as one of the more difficult aspects of GDPR compliance. While privacy notices include the legal basis for processing, many individuals may not understand that not every right is applicable to every legal basis. According to examples from the Information Commissioner's Office (ICO)[1], if companies are processing on the basis of a contract, the individual's right to object and right not to be subject to a decision based solely on automated processing would not apply. Another example from the ICO is that if companies rely on legitimate interests, the right to data portability does not apply.[2] Additional guidance on the lawful basis of legitimate interests would also be very helpful, especially as it was not so commonly used in many EU countries prior to GDPR. These examples ultimately put the burden on data subjects to fully understand their legal rights and put companies in a difficult

[1] "Contract, Lawful Basis for Processing: Guide to the GDPR,"Information Commissioner's Office.
[2] "Legitimate Interest, Lawful Basis for Processing: Guide to the GDPR,"Information Commissioner's Office.

position if users have false expectations when companies are in fact not legally required and/or in a position to fulfil an individual's request. Further guidance on the rights and legal bases for data processing to manage future requests would also be helpful for data subjects. In addition, our member companies would like to highlight the importance of contractual necessity across the board not just in the context of online services. Companies in all industries and sectors including online and offline services, even companies that used to have pure brick-and-mortar business models are now also providing online services and they need to rely on contractual necessity as a legal basis for processing. We recommend more guidance on the necessity for the performance of a contract as a legal basis, going beyond the context of online services.

2. Impact of the GDPR on the Exercise of the Rights

Our member companies are dedicated to ensuring transparency and control for users, with key features including user-friendly privacy tools, updated privacy notices, and easy-to-read dashboards. However, it is difficult to determine the level of detail in the information to be provided to data subjects. Too much detail and the information will inevitably be lengthy and more difficult for data subjects to truly understand. However, data protection authorities may consider that the GDPR information obligations have not been met if there is too little detail, even if that approach makes it actually easier for data subjects to understand.

Many companies have updated and improved their privacy notices since 2018 to enhance comprehension and transparency by providing more details on their practices, avoiding technical and legalistic language, and making the information more interactive and easier to navigate. Below are some key changes:

- An easy-to-read, clear and cleaner look;
- The rewriting of key sections of privacy notices by using clear and plain language, providing more details on the types of information collected, the ways a company may use information, and the privacy controls that users have;
- The notices are refined and information is made available in various forms at different moments when such information is most relevant, tailored to different users, for example using new graphics to communicate key concepts, and, in some cases, new video content to explain key sections. Some companies also highlighted specific text, use illustrations and examples, and integration links to key settings directly into the privacy notice text to make it "actionable," and improve navigation.

3. Impact of Article 7(4) on the Conditions for Valid Consent on a Business Model/Consumers

The main challenge we have observed across the industry is the legal uncertainty as DPAs continue to issue guidance on the use of specific legal bases and enforce against their interpretations of these standards. We would encourage reaching a consistent, clear interpretation of the GDPR in this context across the EU.

4. Complaints and Legal Actions

With regard to the questions on the type of possible complaints against our member organisations, to date companies have experienced complaints mostly in relation to the exercise of data subject rights. In this context, we would further recommend more guidance on key practices such as data subject rights and lawful basis of processing for both the benefits of companies and individual users.

5. Experience with Data Protection Authorities (DPAs) and the One-Stop-Shop Mechanism (OSS)

A genuine, strong cooperation among the EU DPAs will be essential for coherent application and enforcement of the GDPR across the EU. Implementation of the GDPR requires significant resources and work, and will benefit from continued dialogue between companies, regulators, civil society and industry on the development and clarification of the functioning of the one-stop shop and consistency mechanism. Convergence and coordination among the DPAs could improve further. Our members have experienced some challenges in getting timely responses and guidance from the DPAs. They have also noted divergence between guidance from national DPAs and the EDPB guidelines on lists of "high risk" processing operations for which a DPA requires a DPIA.

6. Experience with Accountability and the Risk-Based Approach

The GDPR encourages an approach to compliance based on continuous risk assessment. The implementation of technical and organisational measures has increased awareness about the importance of individuals' trust and the protection of their data. Companies' internal risk assessment documentation and compliance efforts continue to produce results. On the one hand, the GDPR drives a re-thinking of privacy-by-design and takes awareness of data protection to the next level. On the other hand, while driving data management innovation, the GDPR also presents challenges for activities requiring vast amounts of data with little risk and potentially significant benefit for individuals: the training of AI systems in particular seems to clash with the data minimisation concept.

Since before the GDPR took effect, our companies invested considerably in ensuring that technical and organisational data protection measures were robust and up-to-date. In addition to their ongoing work on transparency and user control, businesses have been investing heavily in data security and internal privacy programmes, including strict review processes before any product launch or update, especially in compliance with the requirement to carry out DPIAs for high-risk processing. Some companies incorporated privacy into their company culture, through internal newsletters, screen savers trainings featuring talks with internal and external speakers, and other internal awareness tools to deepen understanding of privacy practices.

7. Data Protection Officers (DPO)

Our members have designated DPOs according to Article 37(1) and the independent nature of the DPO is having a profound impact. DPOs coordinate a structured data protection office with a network of resources, acting locally as the focal and contact point for the relevant DPAs, as well as privacy leaders working on specific processes and streams (i.e. data subject requests, data incidents, transactional work with external clients).

Generally speaking, it is useful that many organisations now have a DPO. Pre-GDPR, not all organisations had in-house knowledge about data protection laws and regulations. The level of knowledge has increased, partially due to the appointment of DPOs. However, there is a certain shortage of knowledgeable DPOs and as a result, the quality across customers and vendors varies.

8. Controller/Processor Relationship (Standard Contractual Clauses)

Our companies have adapted the controller-processor contracts in light of the GDPR mainly to reflect Article 28. These updated clauses were drafted after in-depth discussions with clients and partners and tailored to the specific products involved. Standard language drafted by the European Commission can be difficult to adapt to the wide variety of situations covered by controller-processor relationships across the industries. This language also risks becoming rapidly outdated. In today's age

of Cloud and Software as a Service (SaaS) models, this distinction between "controller" and "processor"is not always clear. The concepts 'data controller', 'data processor' and 'joint controllership' have become increasingly difficult to apply to complex processing operations. Additional, use case-driven guidance on scenarios where suppliers act as joint controllers with businesses would be helpful. Additionally, the content of the controller-processor contracts already achieved a high degree of standardisation.

9. Adaptation/Development of Standard Contractual Clauses (SCCs) for international Transfers

Many ITI members are Privacy Shield-certified. They also rely on the existing SCCs for international transfers where appropriate. Experience with the existing SCCs has been positive, and they often constitute a cornerstone of long-running commercial relationships among millions of parties for many years. Any changes or adaptations to SCCs therefore need to be treated with great caution.

New SCCs modelled after the existing controller/processor SCCs should be made available for processor/sub-processor relationships as, to date, SCCs pursuant to GDPR Art. 46(2)(c), specifically designed to address data transfers between a processor and a sub-processor to or within a third country, have yet to be adopted. Such SCCs would ensure a high level of comprehensibility and accuracy in providing safeguards for the transfer of personal data from EU data processors to non-EEA sub-processors. On the other hand, at present we do not see a need to develop SCCs for specific processing operations. SCCs dealing with broader relationships such as joint controllership would be helpful but not necessarily a priority.

10. Experience or Problems with the National Legislation Implementing the GDPR (e.g. Divergences with the Letter of GDPR, Additional Conditions, Gold Plating, etc.)?

The time required for Member States to update their domestic data protection laws to align with the GDPR has been one issue contributing to the compliance workload. As Member States adopted national legislation, the remaining divergencies from one country to another pose challenges and fragment the EU's single market further. For example, the setting of different ages of consent in different Member States required significant work to ensure that products were updated accordingly.

Another difference that was hard to navigate relates to DPO appointments and notifications. For example, Germany's and Spain's bar to requiring a DPO appointment is much lower than in other countries, with the added compliance burden that represents and there appears to be divergence/confusion as well as to whether global/group of undertakings DPO appointments should be communicated to all the interested DPAs or just to the lead authority.

ITI thanks the European Commission for this opportunity to provide feedback. We reiterate our industry's commitment to trust and privacy throughout the tech ecosystem around the world and look forward to working with the Commission and relevant stakeholders in finding the best solutions.