ITI Promoting Innovation Worldwide

16 April 2020

ITI comments on the two-year review exercise of the General Data Protection Regulation (GDPR)

The Information Technology Industry Council (ITI) is the leading global trade association representing the technology industry. We advocate for policies that promote innovation, open markets, and enable the transformational opportunities that our companies are creating in Europe and beyond. Our members represent the entire spectrum of the technology industry: from internet companies, to hardware and networking equipment manufacturers, to software developers. ITI's diverse membership and staff provide a broad perspective and insight on policy activities around the world.

Our industry shares the goal of safeguarding privacy, and together with our members, we are working with the European Commission and Data Protection Authorities (DPAs) around the world on key data protection and privacy issues, including the General Data Protection Regulation (GDPR). In this context, ITI has recently released its Policy Recommendations for a European Tech Agenda 2020-2024, outlining concrete steps that the EU can take to advance a compelling European tech agenda for the 21st century. This includes several specific recommendations on future privacy policy. The GDPR has catalysed a rethinking of data protection at every level, resulting in wide implementation of industry standards, starting from the engineering and product design phases, to internal documentation of risk assessment and compliance efforts. Companies are adapting their conversations with customers by raising the awareness of data protection globally. Another positive impact is the increased attention in the U.S. to call for a comprehensive federal privacy regime over the past two years. While Congressional progress has been slow, we welcomed the U.S. National Institute of Standards and Technology's (NIST) efforts in releasing their Privacy Framework, which provides guidance to companies on how to comply with privacy regulatory requirements. GDPR has further served as a global benchmark for new privacy regimes and has inspired legislation in Canada, Japan, California, India and Brazil.

Nevertheless, most EU Member State Data Protection Authorities (DPAs) have pointed to a lack of resources and systemic bottlenecks as challenges to efficient and timely enforcement actions within their countries along with resource-intensive cross-border investigations, while at the same time the EDPB recognised that the effective application of the powers and tasks attributed by the GDPR to supervisory authorities are dependent on the resources available to them.

These developments highlight a need to assess how to improve harmonised enforcement of the GDPR across Europe. This submission outlines challenges identified by our member companies in advance of the publication of the European Commission's GDPR report later this year. We hope that our feedback can facilitate a constructive exchange and provide insights to policymakers.

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

Key challenges identified by our industry

Our industry wholeheartedly welcomed the increased harmonisation 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 Computing and Artificial Intelligence. However, we have identified a set of challenges that should be borne in mind in an upcoming annual report on the GDPR:

1. **Enhancing cooperation between Member State DPAs:** The lack of a consistent approach 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. This could be reduced by DPAs by acknowledgement that when investigating cross-border data processing activities, they will take into consideration the requirements and guidelines of the Lead Authority and follow the procedure outlined in Article 56 of the GDPR. A genuine, strong cooperation among the EU's DPAs is essential for a coherent application and enforcement of the GDPR across Europe. We would therefore welcome further clarification and strengthening of the consistency and cooperation procedure among EU DPAs. Moreover, there is also a need for EU DPAs to cooperate with other DPAs outside of the formal cooperation procedure, even in situations where the OSS would not apply. Further, the European Data Protection Board (EDPB) has an important role to play in ensuring that DPAs take a harmonised approach should diverging views emerge. This role also includes the production of harmonised guidance when it is missing.

2. **Upholding the one-stop-shop (OSS) mechanism:** The OSS mechanism is at the very foundation of the GDPR. A central promise of the GDPR was not only to harmonise the substance of data protection across the EU, but also to harmonise the mechanism by which obligations would be enforced. This would reduce administrative burden and provide legal certainty to both companies and individuals. However, there is a risk that this mechanism is being weakened by some DPAs who are challenging the OSS by pointing to bottlenecks and lack of resources for DPAs. In particular, some DPAs are continuing to initiate proceedings, either directly in front of the main establishment without consideration of the lead authority, or in front of local establishments. At the same time, companies have invested significant resources into setting up their European headquarters and compliance programs in anticipation of the OSS mechanism and the EDPB consistency mechanism. The GDPR review should use the opportunity to urge DPAs to comply more thoroughly with the OSS mechanism to ensure that the GDPR is implemented in the most efficient manner. In order to support national DPAs and strengthen the OSS mechanism, national governments must ensure appropriate funding for national DPAs to enable them to carry out their work in the best way possible.

3. **Ensuring high standards for AI applications:** In light of upcoming regulatory approaches to artificial intelligence (AI) and data governance in Europe, we acknowledge that availability of but also responsibility for securing personal data and ethical standards are key, as many promising uses of AI rely on personal data. By leveraging large and diverse datasets and increased computing power and ingenuity, AI developers and other stakeholders innovate across industries to find solutions that will meet the needs of individuals and society in unprecedented ways. We therefore caution against an overly restrictive approach that could risk AI systems being trained on a very restrained set of data due to data protection limitations as this could lead to bias and stifle innovation. At the same time, the GDPR is technology-neutral on purpose and can serve as

a strong foundation to regulate AI, by providing an appropriate regulatory framework to govern processing of personal data in the context of AI. Particularly critical in this context are obligations to ensure fair and lawful processing, transparency, providing individuals with the right to object, along with the incentive for organisations to take steps to anonymise data for these purposes.

4. **Encouraging development of additional guidance:** While we appreciate several guidance documents have been published by the EDPB in the past two years, uncertainty prevails around how the GDPR has to be applied in specific circumstances. We would hence encourage additional guidance from the EDPB to be published on certain topics such as data subject rights, Privacy Impact Assessments and risk-based approach in order to increase legal certainty for companies and securing growth and innovation.

5. **Promoting efficiency, effectiveness and clarity via Codes of Conduct:** As stated above, there continues to be divergence between the national laws of EU Member States, DPAs and outstanding guidance from the EDPB. Approval of Codes of Conduct, in particular of general validity and certification mechanisms, seals and marks would go towards addressing these issues, yielding significant benefit for consumers, businesses and regulators. Codes of Conduct can help create clarity on controller/processor obligations, and lead to gains in efficiency and effectiveness in terms of overall compliance and enforcement. Such mechanisms would ease the compliance burden for large and small businesses alike.

6. **Promoting global data flows:** In light of the growing importance of global data transfers, we welcome the European Commission's work on privacy adequacy decisions and encourage continued efforts to promote global legal frameworks to enable data transfers. The adoption of transfer mechanisms pursuant to Article 46 GDPR, including Codes of Conduct, Binding Corporate Rules (BCRs) and certification mechanisms, is appropriate to enhance the efficiency of international data transfers while ensuring compliance with GDPR standards. We welcome that the ongoing revision of Standard Contractual Clauses (SCCs) included also processor-to-processor clauses. A modular mechanism to replace the existing version of SCCs and a sufficient transition period for companies should be guaranteed. For BCRs, national DPAs need to be equipped with sufficient resources to ensure timely review and approval, in order to create more certainty around data transfers and reduce administrative burden.

7. **Clarifying data processing for Human Resources (HR) purposes:** Employers process a diverse array of employee and applicant personal data. When faced with an employee or applicant data subject request, the GDPR (both the Articles and Recitals) provides limited guidance on responses. For example, Article 15(4) states that access requests may be limited where production would "adversely affect the rights and freedoms of other", but the scope of such rights and freedoms is unduly vague. The recitals only specifically identify such rights as trade secrets, intellectual property and copyrights protecting software. Some EU Member States have further listed the rights and freedoms to be taken into consideration (such as protecting the privacy rights of others), but uniformity is lacking. We suggest more clarity and consistent implementation in this field.

8. **Processing of personal data for research purposes:** In light of the GDPR's risk–based approach, we believe it is important to further explore possibilities mentioned under Article 89 on how the GDPR applies to processing of personal data for research purposes by the private sector. The GDPR assumes a broad conception of research, including technological development,

fundamental and applied research and privately funded research and studies. Academic researchers, not-for-profit organisations, governmental institutions and commercial companies can all carry out scientific research. However, there are concerning differences in implementation at national level with respect to Article 89. The European Data Protection Supervisor (EDPS) in its preliminary opinion on data protection and scientific research recommends that DPAs and ethical review boards intensify their dialogue for a common understanding of which activities qualify as genuine research in the special data protection regime for scientific research under GDPR. We encourage a broad interpretation and enhanced harmonisation in this field across the EU.