DIGITALEUROPE

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

Brussels, 10 February 2017

EXECUTIVE SUMMARY

DIGITALEUROPE, the voice of the digital technology industry in Europe, welcomes the opportunity to respond to the European Commission's questionnaire on the implementation of the General Data Protection Regulation ("GDPR") by industry. DIGITALEUROPE believes that the effective implementation of the GDPR will require a joint effort between all stakeholders **built on mutual trust**. We therefore welcome the initiative of the European Commission to seek feedback from industry on how companies are preparing for GDPR compliance coupled with the hosting of a meeting with industry stakeholders in December 2016 with the intention of continuing the dialogue throughout the implementation process.

As DIGITALEUROPE has referenced in its feedback to the first round of the Article 29 Working Party's ("WP29") draft guidelines, we believe the main objective of all interactions between industry and the European Commission and the WP29 should be to achieve **legal certainty** so that data controllers and data processors of all sizes across the EU clearly understand how their GDPR compliance regimes should be structured. We believe this questionnaire is a positive step in allowing the European Commission to understand that multiple challenges exist across the various business models of DIGITALEUROPE members, particularly when it comes to designing a GDPR compliant personal data governance regime for company-wide systems that need to be used globally. In our response, DIGITALEUROPE has specifically called out the following challenges that are faced by members:

- **Necessity of external counsel** – Members have been obliged to maintain expensive external counsel. This costly exercise is the opposite of the 'cost cutting' envisaged by the European Commission under the GDPR
- **Lack of DPA engagement** – Members seeking DPA engagement/interaction have been met with an overall lack of responsiveness including explicit references to 'no meetings with industry' policies of DPAs
- **Standardised icons** – Members strongly caution the European Commission against adopting delegated acts to produce standardised icons aimed at summarising a company's compliance with the GDPR
- **Controller and processor relationship** – Members have begun adding new elements to their contracts and note that negotiations around liability have become incredibly complex
- **Data breach notification** – Members have warned that they will likely inform DPAs of breaches more frequently than is required/envisaged in the GDPR out of abundance of caution due to potential high sanctions
- **Obtaining consent** – Members and enterprise customers who are processing based on consent are struggling to find effective ways to obtain consent for different processing by the same data controller

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

GENERAL QUESTIONS

1. Are there specific opportunities and challenges in the GDPR implementation in your sector?

DIGITALEUROPE members believe that the implementation of the GDPR provides companies with an opportunity to improve overall data management and data governance, particularly when considering the data inventory and data mapping requirements spelled out in the Regulation.

Multiple challenges exist across the various business models of DIGITALEUROPE members. Overall, the main challenge centres around designing a GDPR compliant personal data governance for company-wide systems that need to be used globally. Such a designation requires immense time, effort and resources to understand how companies can ensure that all data subjects' rights can be satisfied if exercised. In certain cases, profound restructuring of data governance policies will likely need to be envisaged in order to ensure that it is feasible to monitor GDPR compliance across all company systems, databases, offices, etc.

2. Is your organisation cooperating with others in this process and sharing best practices?

To effectively implement and comply with the GDPR, most DIGITALEUROPE members have been obliged to retain external counsel in order to understand best practices across Member States. Such an exercise has not led to the 'cost cutting' which was envisaged by the European Commission under the GDPR. It has had the opposite effect.

Some DIGITALEUROPE members have facilitated sectoral exchanges for their enterprise customers, which have been welcomed. We believe this is potentially an area where the WP29, individual national DPAs and the European Commission can help by organising sectoral exchanges with company experts.

3. What is your experience in cooperating with your data protection authority in that regard?

Cooperation with DPAs varies across the DIGITALEUROPE membership. In general, cooperation has been limited at the moment as many companies and their customers are first trying to reach an acceptable level of GDPR compliance before initiating interaction, while in other cases the interaction (and attempted interaction) has been difficult. In the latter case the experience has been quite unsatisfactory, due to an overall lack of responsiveness, including explicit reference to 'no meetings with industry' policies from several DPAs. After extensive outreach efforts only very few DPA meetings have been held. Moreover, all DIGITALEUROPE members believe that a more inclusive, opened and structured interaction by sector would be very helpful from the DPAs during the planning phase. This would not only be beneficial for companies, but also DPAs as they would get input for the preparation of the guidelines on specific issues.

Furthermore, DIGITALEUROPE members have pointed out that enterprise customers are eagerly awaiting guidance from the DPAs on how to design their compliance. While the publication of the first round of draft guidance on data portability, data protection officers and designation of lead authority have been welcomed, the European data economy is eagerly waiting for the remainder of the draft guidance to be released. Furthermore, DIGITALEUROPE member companies sincerely hope that the feedback provided to the WP29 by all stakeholders

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

will be **carefully assessed and reflected in the 'final' guidance documents**. This will be imperative to building and sustaining a trust-based relationship between regulatory authorities and stakeholders.

SPECIFIC QUESTIONS

1. How is your organisation dealing with the requirements of transparency?

The issue of transparency is one of high importance to DIGITALEUROPE members. While each member company is dealing with it in different ways, overall feedback has shown that enterprise customers have understood that transparency can be viewed as a competitive advantage. However, the delivery method and level of granularity can be difficult to ascertain and varies in many instances. This will need to differ depending on sector and the type of processing involved. Furthermore, specific attention is being paid to reviewing company 'Privacy Statements' including a focus on specific issues such as the legal basis for processing, particularly when consent is heavily relied upon.

2. Are you reflecting about different ways of informing your clients in "concise, transparent, intelligible and easily accessible form"?

As DIGITALEUROPE members work to implement GDPR compliant regimes, many are considering different ways to inform clients although no clear or single system has proven to be preferred. Special considerations have been paid to mobile processing as well as the emerging Internet of Things ("IoT") sphere. Urgent further guidance is needed on this issue however as member companies grapple with providing such information while at the same time not degrading user experience to such an extent that users cease engaging or become impatient. There is no consensus yet as to where the balance lies in such cases.

3. Is your organisation involved in the development of any kind of icons? Are you currently using any?

DIGITALEUROPE welcomes all efforts to make communication of data policies to data subjects clearer and easier to understand. However, we strongly caution the European Commission against adopting delegated acts to produce standardised icons aimed at summarising a company's compliance with the GDPR. Data protection law cannot be summarised into 'Yes/No' answers. Each company is unique when it comes to data processing activities and meets data protection requirements in its own way, which depends to a large extent on how data is actually processed. Some companies have such complex and specific data processing activities that it would be impossible to summarise their data protection practices with icons.

We particularly caution the European Commission against developing icons similar to those proposed by the European Parliament, which chose to focus on minimal collection, minimal or no commercial relationships, sharing of data, and encryption. DIGITALEUROPE firmly believes that the inclusion of such icons are not workable in practice and would make the Regulation no longer technology neutral. Standardised icons applicable to all sectors of the economy are difficult to adapt to the rapid technological developments impacting data processing practices in today's business world. Standardised icons could quickly become outdated or obsolete.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

The inclusion of icons such as those proposed by the European Parliament would also jeopardise the objective of transparency as such icons would be misleading and will not accurately reflect the practices of companies. We are of the opinion that individuals will only be properly informed of data processing practices if companies have the freedom to select and use the right tools to explain with an appropriate level of granularity why they need the data and how they use the data.

Furthermore, the introduction of icons would potentially force companies to incorrectly indicate a violation of data protection law. If an icon is not marked as fulfilled, this will result in making a public statement acknowledging a violation of EU data protection law. We strongly believe that this is conceptually wrong and could have damaging consequences when it comes to transparency and trust from the public. This approach would miss the objective of transparency as it seems unlikely that companies would publicly state via an icon that they do not comply with EU data protection law. Companies would instead likely end up using the 'right' icons to indicate that they comply with EU data protection law even if this is incorrect. Moreover, public trust in effective data protection rules would be at risk if the companies explicitly stating that they do not comply with EU data protection law are not sanctioned.

4. Does your organization have a comprehensive privacy management program? If not: Do you currently work on one? In the case you have one - which changes/adjustments require most work on your side?

Once more, it is difficult to provide one concise answer as privacy management differs across DIGITALEUROPE's members, but overall member companies are re-designing their privacy management programmes and so are many enterprise customers. We refer to the answer provided to question 1 under 'General Questions' as the challenges to re-design these programmes are in certain cases profound. Individuals with a deep expertise in data protection are now necessary for all sectors of the economy. As mentioned previously, the data mapping and inventory effort for many companies is time-consuming and complex, particularly for global organisations. It is challenging for entities to create a new structure and a team across numerous departments that will design, enforce and monitor compliance in an effective and continuous manner. Furthermore, it is worth noting that for smaller entities, particularly European SMEs, the largest question remains whether they will be required to add a DPO and even if not required, whether it is worthwhile doing so.

It should be noted that considerable engineering effort and lead times are required to build for new user rights such as data portability, restriction of processing and the expanded right of objection to profiling.

5. How are you adjusting to the change of the rules concerning the controller-processor relationship? Are you revising your contracts with your processor/processors?

Many DIGITALEUROPE members have already begun adding new elements in their contracts to reflect the requirements of the GDPR. Member companies expect that negotiations around liability will become incredibly complex. Members are receiving requests from customers to answer questions about how their solutions and prospective projects align with the requirements of the GDPR.

6. In the case you are a processor: which measures do you intend to take so as to comply with the GDPR?

For those DIGITALEUOPE members which are involved in 'processor' activities, measures will be determined by the GDPR and by contractual requirements set out by customers. The measures required by customers as of now mostly relate to security and international transfer issues.

7. What is your experience concerning data breach notifications so far? How do you adjust to the new rules?

Once more, it is difficult to summarise the experience of all DIGITALEUROPE members. Overall, to adjust to the new rules companies are looking to maintain a more precise data inventory, increase security measures where applicable, along with more granular and potentially limited access rules.

Some members have also noted that the difficulty in the past has been centred around a lack of uniformity when dealing with data breach notifications. Member companies have high hopes that the lead authority designation can avoid some of the pitfalls which are found in other regions around the globe when it comes to reporting, particularly the US. Those members who have dealt with breach notification requirements in the past, will continue to use their current incident response processes with minor adjustments. However, they warn that they are likely to be over cautious and report breaches to DPAs more than is strictly necessary under the Regulation.

8. Are you processing on the basis of consent? Are you changing/adjusting the way you get consent so as to ensure that it will comply with the new rules?

DIGITALEUROPE members and enterprise customers who are processing based on consent are struggling to find effective ways to obtain consent for different processing by the same data controller. Member companies have expressed that there is an organisational challenge surrounding the single overview of a customer across an organisation where consent may be required for different processing purposes. Furthermore, it is not straightforward to many companies how withdrawal of consent can be managed from a practical perspective.

9. Which mechanism do you use for your international transfers? Do you see any need to adapt the tools you are using or to develop new tools in light of conditions/requirements of your specific industry, business model and/or type of processing operations involved?

DIGITALEUROPE members are using a combination of standard contractual clauses and in some instances the EU-US Privacy Shield. The use of transfer mechanisms in many instances is based upon customer requests. Some member companies believe that BCRs are increasingly becoming attractive for a global organisation although the cost and time process required for approval remains a barrier. All these mechanisms remain effective and do not seem to pose particular problems with GDPR compliance-related projects.

CONCLUSION

DIGITALEUROPE once again wishes to thank the European Commission for providing the European digital technology industry with the opportunity to submit a response to its questionnaire on the implementation of the GDPR. As previously mentioned, it is of paramount importance that data controllers and data processors receive as much legal certainty as possible from the European Commission and the WP29. We look forward to continue engaging with the European Commission and would like to offer the opportunity of a more detailed briefing/feedback meeting with company representatives on their individual experiences. This will provide the European Commission with the opportunity for a more in-depth feedback avenue to fully understand the technical and engineering reality facing data controllers and data processors when seeking to comply with the GDPR.

--

For more information please contact:
Damir Filipovic, DIGITALEUROPE's Director (Digital Consumer and Enterprise Policy)
+32 2 609 53 25 or damir.filipovic@digitaleurope.org

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies.

DIGITALEUROPE ensures industry participation in the development and implementation of EU policies. DIGITALEUROPE's members include 60 corporate members and 37 national trade associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Force Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: ICT IRELAND
Italy: ANITEC
Lithuania: INFOBALT
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK