29 April 2020

GDPR roadmap: Feedback from JBCE

JBCE's submission to the European Commission's request for feedback on the two-year review exercise of the General Data Protection Regulation (GDPR)

Introduction

The Japan Business Council in Europe (JBCE) is a European association representing over 80 multinational companies of Japanese parentage in EU policy discussions. Our members are active in Europe across many sectors, including digital, information and communication technologies, electronics, automotive, pharmaceuticals and chemicals. JBCE aims to be a bridge between the EU and Japan to strengthen ties and cultivate understanding among European decision-makers of the contribution of Japanese companies to Europe.

Feedback

JBCE's Digital Innovation Committee (DIC) thanks the European Commission for providing the opportunity to provide feedback on its GDPR evaluation roadmap.

The GDPR continues to hold a number of positive aspects for JBCE's members, most notably, facilitating global data flows, improving global standards for privacy and data protection, and bringing some clarity to the application of data protection rules in the European Union. However, considering the significant resources mobilised by JBCE's members to ensure they are fully compliant, there remain both: i) challenges in interpreting the GDPR, ii) and a need for greater harmonisation.

I. Challenges in interpreting GDPR

Specific points to raise include:

- **Guidelines on Data Protection Impact Assessments (DPIAs) and cloud service providers**. The JBCE would appreciate if the EU could prepare a set of common guidelines for global cloud service providers. These guidelines could give a safety approval for those providers. Especially as global cloud service providers have not always provided full replies to the questions in the DPIAs, making it more difficult for JBCE members to properly evaluate the security risks.
- **Simplifying Binding Corporate Rules (BCR)**. Considering the fact that Standard Contractual Clauses (SCC) are forcing Japanese companies to take on a heavy workload, despite the adequacy decision between the EU and Japan, BCRs should be a desirable option in the long-term thanks to its comprehensiveness. However, it takes approximately 15 to 24 months to secure the necessary approvement of the rules - a delay that could act as an obstacle to the widespread use of these measures. With that in mind, JBCE would appreciate if the EU could consider measures to simplify the procedure and shorten the necessary time required for BCR certification.
- **On Legitimate Interest.** The JBCE would ask the European Commission to oversee and monitor the interpretation of the Legitimate Interest principle by National Data Protection Authorities

(DPAs) to ensure a harmonized approach. The JBCE would appreciate the EDPB to provide guidelines ensuring the right balance between citizens' privacy rights and the legitimate interest of data processors. Avoiding situations in which Member States introduce national requirements on top of the GDPR would be the key objective here. It would also be important not to exclude *a priori* commercial interests and profit maximization from the "three steps Test" (Purpose test, Necessity test and Balancing test).

- **On the use of bio-metric data**. The JBCE appreciated the guidance provided by the EU Data Protection Board on the use of biometric data in the context of video recording, especially for data processors as there remains a very fragmented approach between EU countries.
- **Securing compliance with other rules that are of important public interest**. The GDPR has created problems for companies trying to secure compliance with other rules that count as important public interest. For example, tackling bribery and corruption. To avoid involvement in corrupt practices, many public enforcement agencies within the EU and outside (in the U.S. notably), expect their companies to have robust compliance programs in place with a proper screening of business partners. However, if such screening should uncover criminal convictions for private individuals, even if this is only reporting in public news media, this could pose problems under national law where processing of personal information concerning criminal convictions are only authorized in very narrow circumstances or authorized only for some sectors (such as in the financial sector). In a few Member States, such as Denmark, processing of such information is possible where there is a strong legitimate interest that clearly overrides the interests of the data subject. This should be the case across the entire EU, not just for bribery prevention, but for any other important public interest, such as avoiding fraud or similar.

II. The need for harmonised implementation

Specific points to raise include:

- **Cooperation among DPA**. Strong cooperation among DPAs is essential for a coherent enforcement of the GDPR. JBCE's members appreciate the efforts made by the European Commission to avoid conflicting interpretations between DPAs, but we still see a lack of harmonisation and diverging national interpretations of Europe's data protection rules. JBCE members will continue to support the existing implementation dialogue and processes underway at national level as much as possible, but we underline that progress should be made towards a more coherent and harmonised European solution to implement the GDPR.
- **The benefits of pan-European Codes of Conduct and certification mechanisms**. Codes of Conduct can be effective in helping companies throughout the supply chain, regardless of size and risk profile, in demonstrating their compliance with the GDPR's principles. The current approach of decentralising Codes of Conduct according to national criteria has limitations. It risks weakening the effectiveness of adoption because of its higher cost and timing constraints, obstacles that are felt especially strongly by the SMEs that depend on JBCE's members for continued prosperity. The GDPR was always envisaged as a business enablement mechanism, and for these codes to be truly effective they should span multiple industry sectors in which processing operations are similar. Pan-European codes would ensure a greater ease of adoption and help ensure a more consistent approach. Moreover, greater harmonisation

across the EU is critical for the successful adoption of certification mechanisms. The EU can adopt a certification programme that simplifies adoption requirements; allows for risk-based differentiation based on, for example, the size of the organisation; and earn international recognition. Duplication and fragmentation risk diluting the effectiveness of this mechanism, making widespread adoption by the business community unaffordable. EU-wide harmonisation can help generate the scale necessary for JBCE's members to see a real value in certifying.

- **More harmonised rules on cookies**. Companies operating across the EU continue to see diverging guidance from national DPAs on the use of cookies (consent), partly related to a patchy implementation of the ePrivacy Directive, with some Member States, including Germany, having yet to implement all of the Directive's requirements. This increases the burden on companies.
- **More harmonised approach on data breach notifications**. Currently, each DPA employs its own method on how companies can submit data to them. This includes different submission modalities (e.g. web page, e-mail, word document) and varying requirements for information disclosure, with some DPAs requiring detailed and granular submissions, some not. These different approaches significantly increase reporting time and administrative costs. Ideally, all DPA should request the same information with the same level of information granularity. Ideally, organisations should be able to submit details in a human-readable form (e.g. PDF) but also in a machine-readable format (e.g. XML). Allowing organisations to automate submission processes, bringing benefits to everyone. Organisations will know exactly what information they need to collect, submission process can be streamlined and DPAs will also be able to streamline their processes. The ultimate solution would be that DPAs seamlessly share information between them so that an organisation can use any DPA to report issues irrespective of which Member State is involved (in line with one-stop-shop idea).
- **Stronger oversight at EU level**. Greater harmonisation and oversight at EU level, with a "EU Data Protection Office" would present some advantages for companies operating in the EU. National DPAs would be able to refer questions or queries more easily, and the authority would be able to review all cases, thereby making it possible to appeal an unjust decision, or submit mitigating evidence after a fine has been issued. For example, a company could typically have servers located in Germany, be incorporated in the Netherlands but witness an incident in the UK. The company would face uncertainty as to whether to report the incident to the UK or Dutch DPA. An overall EU authority would help avoid this problem.