JBCE Recommendations for the e-Privacy Regulation

29 August 2018

The Japan Business Council in Europe (JBCE) respectfully submits these recommendations on the proposed e-Privacy Regulation (ePR - COM(2017) 10 final)[1] to the attention of the EU Institutions. It is a reality that the EU regulatory framework must adapt to accommodate the fast pace of technological development and evolution. JBCE commends the efforts of the European Commission to modernise data protection frameworks to establish the EU as a leader in the digital data economy. With the passage of the General Data Protection Regulation (GDPR) in May 2016, the Commission saw a need to align existing privacy and confidentiality rules in the electronic communications sector with this new regime and in early 2017 put forth a proposal for an ePrivacy Regulation[2] to replace the former Privacy and Electronics Communications Directive[3].

Traditionally this directive only applied to providers of electronic communications services. However, the scope of the current proposal is much broader and includes other segments of the digital economy, including several members of JBCE. Accordingly, JBCE seeks to support the deliberations of the European Parliament and the Council by offering the following reflections on potential areas for improvement to the legislation.

Transmission of Personal and Non-Personal Data

Similarly to the version put forward by the Council, JBCE distinguishes between the "transmission layer" for M2M communications, (e.g., communication being sent over a telecoms network) and the "application layer" (e.g., when the machine carries out a command received through a transmission). We believe that the ePR should only apply to the former. In the current text, the wording on transmission and application layers lacks clarity, risking broad interpretation and diverging forms of implementation. For instance, it is not apparent in the proposal where the ePR takes effect and where the end point is situated. By definition, once data is received it is no longer being transmitted but instead offering a service or command that is separate from the underlaying network.

Under Recital 15 of the draft ePR, the prohibition on processing of electronic communications data without a legal basis should apply only to data "in transmission". Such prohibition is appropriate as it envisages to protect users against interception or scanning of communications in transit. However, this limitation is not properly reflected in Article 5. The fact that this article distinguishes between processing from other activities (e.g., listening, tapping, monitoring and scanning) adds to the likelihood that Article 5 could be misinterpreted as also applying to data "at rest". Moreover, the report[4] adopted by the Parliament in October 2017 expanded the categories of data covered by the ePR by specifying that it covers communications data, whether in transit or at rest. This contradiction contributes to confusion while overlapping with the GDPR, which already covers data "at rest". Though the Recital shows the Commission did not intend for the ePR to apply to data at rest, JBCE stresses that the language needs to be clearer and that the Council should reject the extension suggested by the Parliament.

Should the result of the ongoing legislative process keep M2M communications as part of the material scope of the ePR, it is important to avoid new anti-competitive scenarios. Article 7, perhaps unintentionally, allows telecom operators to keep data after it is transmitted, provided it is anonymised. They would therefore be able to aggregate these valuable data and sell it to third parties with huge benefit to them. In our view, the use of such anonymised data should be agreed in a B2B context and not be an automatic advantage given to telecom operators simply for having anonymised the transmitted data.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN
[2] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241
[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML
[4] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0324+0+DOC+XML+V0//EN

JBCE recommendations:

- **Provide clarity to the material scope of the ePR by excluding the "application layer" of M2M communications from Article 2 and Recital 12 of the draft ePR.** The purpose of the ePR is to protect the confidentiality of information of natural persons in the provision and use of electronic communications services. As the application layer of M2M communications does not represent an electronic communications services, it should not fall within the scope of the ePR but instead of the GDPR.

- **Clearly exclude non-personal data from the scope of the ePR.** Communications that are disconnected from natural persons do not present any privacy or confidentiality concerns and should therefore fall outside the scope of the ePR. In the absence of such clarification, the ePR will inadvertently capture countless smart devices and IoT applications (e.g. smart homes and appliances) in its scope. We welcome the Parliament's Report which rectifies this weakness by restricting the principle of confidentiality to M2M communications only when related to a user.

- **Revise Article 5 to explicitly state that the ePR applies to data "in transit" and prohibits interception, scanning and other interference.** We propose the following wording:

"Transmission of personal data in Electronic communications ~~data~~ shall be confidential. Any interference with ***the transmission of personal data in*** electronic communications ~~data~~, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of ***personal data in*** electronic communications ~~data~~, by persons **or entities** other than the end-users, shall be prohibited, except when permitted by this Regulation"

- **Revise Article 7 to ensure a level playing-field between the provider of electronic communications services and the data sender or the intended recipient(s).** We propose the following wording:

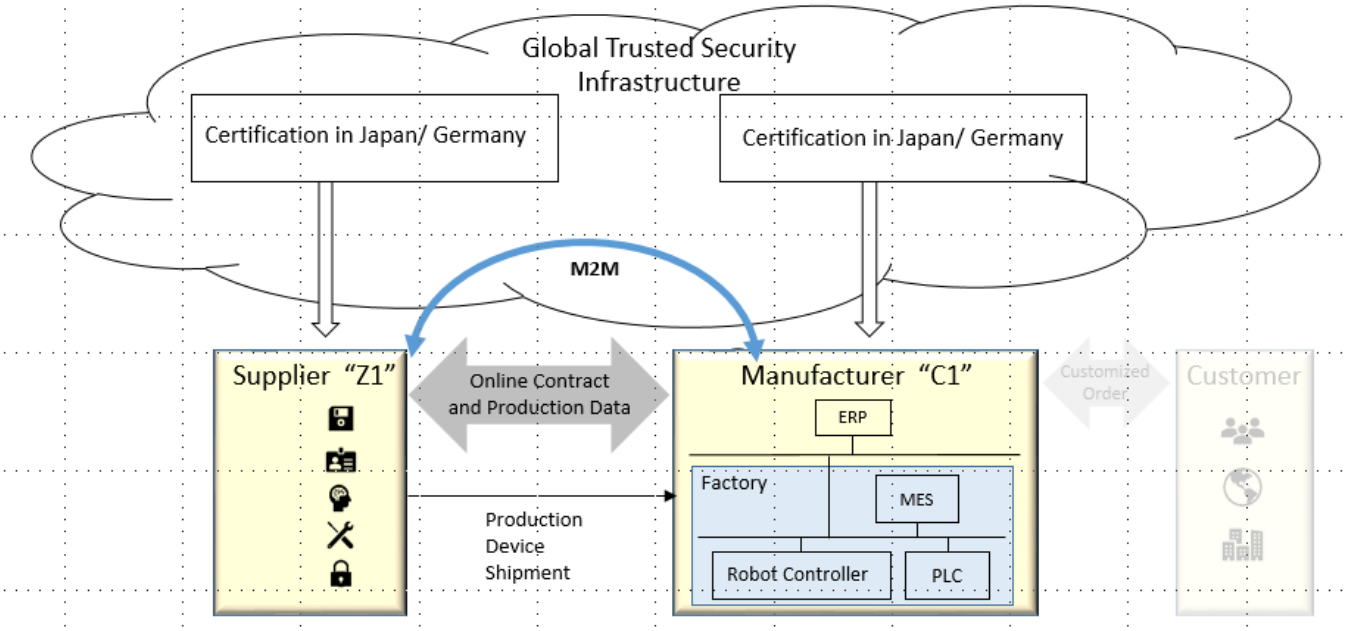
"Without prejudice to point (b) of Article 6(1) and points (a) and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications content or**, upon agreement with the involved parties, namely the data sender and the intended recipient or recipients,** make that data anonymous after receipt of electronic communications content by the intended recipient or recipients."

Please, find below a few use-cases to support our recommendations.

Use-case: Cross-company/country communication between two machines within a supply chain between suppliers

Secure (company-wide/ cross-company) operations require trust and legal certainty between all parties involved. Each manufacturer wants to give his customer clear, comprehensive and reliable information about the properties of the system, product and data delivered. M2M communications are based on secure, legitimate and appropriate production data as an **overall process, independent of the terms "application" and "transmission"** - this view is based on cross-company, cross-border and cross-sector value chains in **Industry 4.0 manufacturing** or **Connected Industries.** Within a supply chain we don't need any new rule, any "Service Provider" in this value chain is part of the secure channel as described below example.

Example:
The Japanese supplier "Z1" has been issued with a corporate certificate and the German manufacturer "C1" has been issued as well with a corporate certificate to identify themselves as well as securely establish an online contract to produce a device according to customer-specific requirements. Due to the customer's demand of a product, Manufacturer "C1" provides data from its machine to the machine of Supplier "Z1". The machine of the Supplier "Z1" processes non-personal data and produces the device for the customer. Both machines of Manufacturer "C1" and Supplier "Z1" exchange at the end of the production the customer-specific production data of belonging to the device.



Use-case: limitations to process data make it challenging to improve services and customers

Printer manufacturers use metadata to manage the networks of printers and offer better services to current and future customers (e.g. software updates; improving the security of the devices). If the ability of manufacturers to process metadata from printers is limited, it will be challenging to further improve their services to customers.

Use-case: Unfair competitive advantage given to service providers once data is anonymised

Company A, holding the data of a connected car, transmits data to Company B, using a provider of electronic communications service. According to Article 7(1) the service provider can decide to retain for free the data by anonymising them. But even in an anonymised form, those data still retain a huge value that would put their holder in direct competition with both Company A (as telecom operators will be able to collect data from several other companies/cars and aggregate all in huge databases for further AI elaboration) and Company B (they may use the data for the same use case). Eventually the service provider could even re-sell the anonymised data and get extra benefit from them.

Coherence with the GDPR

In addition to the example of data "in transit" versus "at rest" described above, there are **other aspects of the ePR that could be improved to align with the GDPR**. For instance, the ePR proposes a consent-only model, whereas the GDPR recognises other tools for processing as long as safeguards are in place, including legitimate interest. This limits the capacities of EU industry to develop new businesses, benefit from big data processing and improve customer service in innovative ways. The Parliament failed to correct this in its Report, in fact the Parliament proposes to restrict processing even further. JBCE calls on the Council to be attentive to the conditions for processing provided for in the GDPR, which represent a workable and more balanced data processing solution and bring the texts back into alignment. If all data processing relies on consent this can cause "consent fatigue" or make consent meaningless overtime as users will not understand what is relevant as everything is based on the same model.

JBCE welcomes the latest compromise text proposed by the Austrian Presidency that recognises the need for a regulatory framework that is flexible enough to enable the development of innovative services. To achieve this, the text takes inspiration from the GDPR and has introduced a possibility for further compatible processing of electronic communications metadata.

JBCE recommendations:

- **Take inspiration from the GDPR and introduce the same processing conditions.** This should include "legitimate interest" as a legal basis for processing and compatible further processing. These in any way compromise the protection of personal data as in order to be operated the rights and interests of individuals cannot be infringed. By failing to align the ePR with the GDPR in this context, businesses will have to rely on end-users consent alone as a basis for processing activities with a stifling effect on innovation.

Please find below a few use-cases to support our recommendations.

Use-case: Cooperative Intelligent Transport Systems (C-ITS)

According to the draft ePR, vehicle-to-everything (V2X) communications may be in the scope of ePrivacy. To control quality, the original equipment manufacturer (OEM) would need access to V2X communications metadata. A consent-only model to process data would turn this frequent activity impractical and potentially render the deployment of C-ITS applications very complicated.

Use-case: Storage and processing of data or their collection from the vehicle as "terminal equipment"

Connected vehicles are considered "terminal equipment" (like a computer or a smartphone). Article 8 of ePrivacy prohibits the use of processing and storage capabilities of terminal equipment and the collection of information from terminal equipment without end-users consent. OEMs would have to ask consent from the data subject to process vehicle data in a number of cases that are normally covered by other legal grounds in the GDPR (e.g., "legitimate interest" for complying with product safety and product liability legislation, or for performing software updates in vehicles, the performance of contract such as for transmitting data to provide connected services).

Terminal equipment

With regard to terminal equipment, JBCE notes that the **concept is not clearly defined in the text**, rather, the draft ePR refers to secondary EU law. This is problematic, not in the least because the secondary law referenced are directives (cf. the Radio Equipment Directive) and therefore implemented differently across the EU. Furthermore, the fast technological evolution around IoT requires caution when deciding on definitions that would need to cover tools, equipment and technologies that are diverse in their nature and dynamic in their evolution. Without an agreed technological and future-proof understanding of what terminal equipment is, the ePR risks to be implemented either more conservatively or more progressively across Europe, jeopardising the harmonised level of protection granted to these equipment and, consequently, to their users envisaged by this Regulation. The report adopted by the Parliament in October 2017 begins to address this, amending the text to make the ePR applicable not only to information related to the terminal equipment of end-users but also to information processed by such equipment, helping to define the material scope more precisely.

Another issue is presented by Article 8(1), which **prohibits the collection or storage of information** on terminal equipment unless certain conditions are met, including consent. But nowadays, most data processing activities use "processing and storage capabilities of terminal equipment" making it necessary for controllers and processors to comply with this prohibition. However, processing is performed for many legitimate purposes (many allowed under different legal basis in the GDPR) including for non-privacy-invasive causes such as improving security, enabling technical functionalities and develop innovative services and products. Indeed, unless information about the functioning of devices is allowed to be processed, it can be impossible for terminal equipment manufactures to carry out important supportive services such as updates, diagnostics or troubleshooting.

JBCE recommendations;

- **Guarantee an implementation period once the ePR is adopted during which, similarly to the GDPR, the European Data Protection Board issues guidelines interpreting concepts such as terminal equipment in a technological neutral and future-proof manner.** These guidelines should be produced in consultation with stakeholders.

- **Delete Article 8(1) or recalibrate the scope of terminal equipment captured by bans on information emitted and recognise in the ePR that not all terminal equipment is personal, nor is it sensitive. JBCE recommends the co-legislators to consider a more flexible and granular approach based on the recommendation stated above that non-personal data should be excluded from the ePR.**

Please find below a few use-cases to support our recommendations.

Use-case: Future-proof definitions for rapidly evolving technologies

The majority of cars used today are "traditional vehicles" with no data transmission, despite the massive use of in-vehicle electronics. To help these vehicles transmit data, an "alien" tool is necessary, capable of harvesting data from the BUS and deliver to a recipient. These dongles could represent a terminal. New vehicles under development will have a built-in technology to transmit these data, so that the car itself will be regarded as a terminal. Thinking further about the possible evolution of vehicle connectivity, it would not be impossible to imagine a future in which the connectivity and transmission capabilities could be channeled through an enhanced smartphone capable of replacing all the computational capability of the onboard computers. The smartphone then will be the terminal equipment. From the above it is clear that for the same product, technological development represents an evolution that brings traditional "mute" products to start "talking" (transmitting) with many possible alternatives, difficult to predict beforehand.

Conclusion

JBCE is in full support of the European Commission's efforts to create a data protection framework that reflects the needs of a rapidly changing digital economy. We likewise commend the decision to design a Regulation to continue the harmonisation of regimes across the EU began by the GDPR. As these Regulations must ultimately reinforce each other, JBCE calls for an efficient legislative process so as to diminish uncertainty and avoid a long time gap between the GDPR implementation and the ePR entry into force. In no way, however, should this efficiency come at the cost of developing a robust legal text.

The points above illustrate that there is still room to improve the ePR to maintain coherence with the GDPR and propose proportionate and sensible measures for M2M communications and terminal equipment. JBCE encourages the co-legislators to consider these points to significantly strengthen the text. To further support a smooth transition for DPAs and business, JBCE sees value in an implementation period with appropriate guidance from the European Data Protection Board.

About JBCE

The JBCE represents the interests of 84 multinational companies of Japanese parentage operating in the EU, with members operating across a range of sectors, including electronics, wholesale trade, precision instruments, pharmaceutical, railway, textiles, glass, automotive, and chemical manufacturing. The key goal of JBCE is to contribute constructively to EU policies, drawing on the expertise and experience of our member companies. Building a new era of cooperation between the EU and Japan is the core of our activities.