SP2C Les entreprises de la relation client externalisée

European Data Protection Board

December, the 21th 2021 in Paris

About Public Consultation : "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data"

SP2C brings together the main French outsourced contact center companies in outsourced customer experience. Our members employ more than 86,000 people and operate in a market of nearly 3 billion euros in turnover. The vocation of SP2C is to promote and enhance our profession, defend its usefulness and improve its influence.

SP2C thanks the European Commission for the opportunity to provide comments on the EDPB on their recommendations 1/2020. Indeed, in an increasingly international and digitized context, and in addition to the approach of Brexit, it is essential for companies to quickly have a stable, secure and efficient legal solution. It allows the maintenance and continuity of transfers of personal data outside the EU, as long as the Standard contractual clauses remain the tool most used by companies for transfers outside the EU. It is also essential for companies to have proportionate mechanisms, based on on the key principles of the GDPR and taking into account political, judicial and above all economic. However, as it stands, the draft recommendations of the European Committee for the Protection of data (EDPB) does not meet these objectives and raises serious concerns within companies.

As the GDPR takes a risk-based approach by empowering companies and making them allowing them to carry out analyzes of their needs and risks in order to adopt the security or appropriate guarantees, the draft recommendations call into question this approach by the risks. However, this approach is fundamental for companies because it makes it possible to assess the risks for their business and to choose a solution that meets their needs. By imposing measures on set up, companies are limited in their freedom of choice of their co-contractors.

Indeed, the adoption of expensive and not necessarily appropriate technical measures may discourage a company from contracting with a service provider located outside the EU due to a cumbersome process and expensive. The company can therefore no longer decide on policy and governance for data that it holds since it is therefore constrained in the choice of service and provider. The risks should be assessed on a case-by-case basis and include the likelihood of a request for access and interference by a foreign government. It is up to the company to take into account the sensitivity of the data concerned and the measures to be put in place to protect the data it holds. However, the EDPB has adopted a very strict approach considering that data transfers to countries third parties should not take place (or under conditions almost impossible to implement) if the laws of information from these countries is not compatible with European standards.

The draft recommendations do not distinguish between the purposes or the different categories of data. This differs from the general approach taken by the GDPR, which distinguishes the processing of "classic" personal data processing of "sensitive" personal data(art 9). Likewise, the regulation also recognizes that security risks, to which personal data is subject, and the measures that companies must define and set up accordingly, vary depending on the nature of the data, the sensitivity of this data and risks for the data subjects.

Otherwise, the draft recommendations of the European Data Protection Board set out as a key to vaults technical measures, to the detriment of organizational or contractual measures. The text, and in particular paragraph 48, establishes the primacy of technical measures over organizational and contractual measures when the national law of a third country allows the authorities public access to personal data, without appropriate guarantees.

However, technical measures, such as encryption, are expensive, difficult to implement and do not necessarily defeat either the access of foreign public authorities to data, or the problems incompatibilities of laws and therefore contradictory obligations to which companies are subject.

✓ **Measures can be difficult to put in place**: not all technical measures are not equally effective. The EDPB recommends encryption where only the client holds the data decryption key (“Bring your own key”). That causes a problem in the event that the customer uses his data with an external service provider. In this case, a company that exports data is forced to implement encryption and decryption mechanisms independent of the latter (if the client wants to have this data at any time). Such a system would incur software development costs very important additional data for companies exporting these data. Indeed, although encryption is often the most relevant option to protect data, this option may appear very expensive and unsuitable for some data types and some business models.

- ✓ **Costly measures**: in the same way, these technical solutions and in particular the Encryption mechanisms that are not "off the shelf" involve high costs for companies that export data, especially if it needs to be done constantly. The cost of encryption includes both the purchase of the solution and the interoperability with the entire company IT system. These costs will have consequences for all players wishing to store data. These mechanisms do not are therefore, not within everyone's reach and imposing the use of such measures would penalize strongly smaller structures. VSEs / SMEs will prefer to take measures basic encryption on shelves, less expensive but technically insufficient, as they cannot afford such additional costs for their data.

- ✓ **Measures that do not correspond to operational realities**: impose the use of technical measures such as systematic encryption do not take into account the realities technical, operational and economic, all the more for very small businesses. Finally, it is technically impossible to ensure completely foolproof encryption over the long term. Howewer, use cases 1 and 3 of the EDPB recommendations use the term "flawless" which could be dangerous in terms of liability for data exporting companies.

So, if encryption is required for some data, it should not be enforced systematically to companies in the context of transfers of personal data outside the EU. Againly, applying the risk-based approach, it is up to the company to determine the data and the circumstances that require encryption. In some cases, encryption is not everything simply not suitable for processing because the data must be available in clear. This will result in slowing down the development of French and European companies internationally. It is therefore essential that the EDPB grant greater flexibility to companies in implementation of data transfer mechanisms outside the EU.

In the long-term, it will negatively impact Europe's geopolitical influence, turning us inwards and risking retaliation from other regions. While a challenging task, the EDPB's current approach threatens Europe's bid to become "fit for the digital age" to the detriment of strengthening Europe's data economy, maintaining trust in digital services, ensuring high cybersecurity capacities and leading in Artificial Intelligence (AI). So, SP2C call for the EDPB to rethink its approach in order to better align with the GDPR, recent CJEU jurisprudence and the Commission's (draft) SCCs in order to safeguard Europe's data flows in a more pragmatic manner. We encourage:

- Following a risk-based approach that takes the full context of data transfers into account;
- The possibility to continue relying on contractual and organisational measures;
- Developing workable technical solutions (rather than overreliance on encryption).

Counting on your understanding, we remain at your disposal.

Contact :

Caroline Adam
General Secretary
Secretaire-general@sp2c.org
Phone : +33 / 06 13 62 40 13