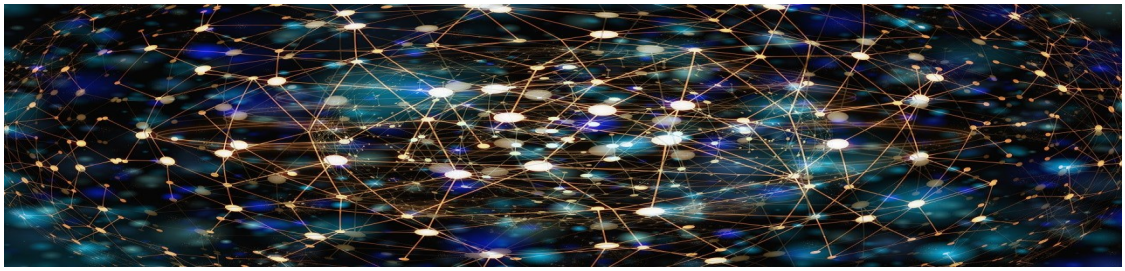
AMMOURA



PROTECTION OF PERSONAL DATA - Practical Issues

INSIGHTS

The General Data Protection Regulation (GDPR) has been applicable in the European Union since 2018, having introduced several changes in terms of the protection of personal data.

Companies and citizens had to adjust to the new applicable regulation, under penalty of being charged heavy fines, which can reach EUR 20 million or, in the case of companies, up to 4% of their annual global turnover, depending on the whichever is higher.

But since GDPR has been in force, some practical questions are frequently asked, such as those related to the confluence between the right to portability and the right to erase personal data. Regarding the right to portability, the transfer of data related to personal preferences that are obtained and registered by means of algorithms, for example, is also discussed.

As for the transfer of personal data to companies residing in third countries without an adequate level of protection, the recent decision of the National Data Protection Commission (CNPD) within the scope of the 2021 Censuses is addressed.

We raise and clarify some of these practical questions below.

PORTABILITY WITHOUT ERASING?

Anyone, as a owner of personal data, has the right to data portability. This means that anyone has the right to receive the personal data that you have provided to a certain company and to request its transfer to another company.

Without prejudice, this right can only be exercised if the personal data have been collected in a structured format, in common use and automatic reading, in a contractual context or based on the consent of the owner of such data, and if the processing is carried out by automated means. .

Portability is useful when the owner intends to use his personal data already collected and processed by a certain company, to initiate or complete a contractual relationship with another company that will proceed with the processing of such data, with the repetitive collection of data being unnecessary.

But contrary to what it might seem, the portability of the data does not imply the elimination of it in the company that transfers it.

Even if the data is transferred to a new company, under the terms of portability, if the data subject does not expressly request the elimination of such data, the initial company may proceed with the respective treatment.

Note that the owner has the right to have his personal data deleted. In turn, the controller has an obligation to delete, when one of the following reasons applies:

a) Personal data is no longer necessary for the purpose in question;

b) The owner withdraws the consent on which the processing of the data is based;

c) The owner is opposed to the treatment;

d) Personal data has been processed illegally;

e) Personal data must be erased in order to comply with a legal obligation;

f) Personal data were collected in the context of the provision of information society services in relation to children.

If the owner exercises the right to portability of personal data, without exercising the right to delete such data, the company remains legitimate to the treatment of all such personal data.

Also within the scope of the transfer of personal data, data relating to the owners' preferences may be included, collected through algorithms, registered and processed for various commercial purposes, namely on e-commerce platforms.

The algorithms, or the respective systems and programs, may eventually be protected by industrial property rights, so it is questioned whether the company that performs the data processing may refuse to transfer them to any other company designated by the data owner .

It should be noted that the right to portability is not an absolute right. The rights and freedoms of third parties are not prejudiced. In any case, there is no guarantee that a company will be able to refuse to transfer data on the grounds of the protection of industrial property.

Another interesting point concerns the transfer of personal data to third countries without an adequate level of protection, in the scope of portability. What happens if the owner requests the transfer of data to a company resident in one of those countries?

Data transfers to third countries (or international organizations) can be carried out if the European Commission (EC) has decided that such a third country ensures an adequate level of protection.

In the absence of an EC decision, controllers (or subcontractors) may transfer personal data to a third country if adequate guarantees have been provided. This can be done through standard data protection clauses, for example.

When there are no adequate guarantees, the data subject must explicitly check his consent to the transfer. For this purpose, the company subject to the transfer under the right to portability, must inform the data subject about the possible risks for himself.

TRANSFER TO THIRD COUNTRIES WITHOUT ADEQUATE PROTECTION?

INSIGHTS

The limitations on the transfer of personal data are accentuated for third countries without an adequate level of protection, that is to say, which are not covered by laws and regulations similar to those in force in the European Union.

A paradigmatic case of these limitations refers to the recent decision by CNPD, which ordered the National Statistics Institute (INE) to suspend the sending of personal data obtained through the 2021 Census to a company based in the United States of America (USA).

The foreign company in question is subject to US surveillance legislation for national security purposes, including the legal obligation to provide unrestricted access to US authorities to personal data, and is prohibited from informing the respective data subjects.

However, the Court of Justice of the European Union (CJEU) recently considered, through the Schrems II Decision, that such legislation implies non-proportional interference in the fundamental rights of data subjects, and a level of data protection essentially equivalent to that guaranteed in the EU is not guaranteed.

Indeed, under its powers, the CNPD intervened and ordered the suspension of the sending of personal data to the USA.

This severe intervention, to which fines may be added, may occur in other similar situations, so it is clear that companies and data controllers must consider these implications when entering into contracts with companies based in third countries, ensuring that they comply with fully all applicable legal regulations.

Article written in accordance with the legislation in force on 21 May 2021.