ONTIER

PRIVACY AND DATA PROTECTION INTERNATIONAL TEAM

06th December 2016
#4

Index

1. Territorial Scope 2. Consent 3. Genetic Data and Biometric Data **4. Rights of the data subject** 5. Profiling 6. Controller and Processor 7. Data Protection by Design and By Default 8. Data Protection Impact Assessment 9. Records of Processing Activities 10. Data Breach 11. Data Protection Officer 12. Codes of Conduct 13. Certification Bodies 14. Transfer of Personal Data 15. One Stop Shop 16. Independent Supervisory Authorities 17. European Data Protection Board 18. Remedies, liability and penalties

NEW RIGHTS: RIGHT TO BE FORGOTTEN AND RIGHT TO DATA PORTABILITY

In addition to the maintenance of the traditional rights at the disposal of the data subject (right of access, right to rectification, right to erasure and right to object), the GDPR introduces two new rights: the right to be forgotten and the right to data portability. Both are closely related to the traditional rights and even may be considered new manifestations or evolutions of some of them.

Current situation

Directive 95/46/EC establishes consent as one of the main legal grounds that legitimize acts of processing of personal data. Furthermore, the Directive grants to the data subject several rights that allow post control or modulation of the acts of processing carried out by Data Controllers or Data Processors. They are the rights of access, rectification, erasure and objection. Thus, the data subject is able to know which data is being processed, to ask for an update, to object to the processing for certain purposes or to request the erasure if the Data Controller fails to comply with the Directive. Although these rights are not absolute as there are situations in which the Data Controller is not obliged to grant them, they pose a manifestation of the protective nature of the data protection regulation.

What's new?

The new GDPR recognizes two new rights for the data subject, which also consolidates his/her power to decide which companies, and for what purpose, can process his/her personal data. They are: (i) the "right to be forgotten" and (ii) the right to data portability.
Article 17 of the GDPR regulates the "right to be forgotten", which codifies the right of cancellation expressly recognized by the European Union Court of Justice in the case of *Google Spain SL and Google Inc. v Spanish Data Protection Agency and Mario Coasteja Gonzalez (*C-131/12). The court ruled that search engines should remove those results that link to inaccurate or outdated content upon application of the data subject, provided that a public interest does not exist. The GDPR incorporates this right to the apply to all Data Controllers and not just search engines.
A data subject is entitled to request the erasure of his/her personal data in any of the following situations: (i) when personal data is no longer needed with respect to the purpose for which it was collected, (ii) when the data subject withdraws consent or oppose to certain acts of processing, provided that there are no other legal ground that legitimizes these acts of processing, (iii) when personal data have been processed unlawfully, (iv) when personal data must be deleted to comply with a legal obligation, or (v) when data has been obtained in relation to services offered to minors.
Once the right has been exercised, if the personal data of the data subject has been made public by the Data Controller, it must adopt measures, including technical measures, to inform other Data Controllers and Data Processors who are processing the data about the request, so that they can delete any links or copies of the data.
The right to be forgotten will be denied when acts of processing were justified by the exercise of freedom of expression and information, the public interest, the need to comply with a legal obligation or the exercise or defense of claims obligation.
The GDPR also introduces the right to data portability, which implies that any data subject may request the Data Controller (provided that it’s a service provider), to deliver all his/her personal data at its disposal in a structured, commonly used and machine-readable format. For this, two requirements must be met: (i) the processing is carried out automatically and (ii) the legal grounds for processing are either the data subject's consent or it is needed for the execution of a contract to which the data subject is a party to. The data subject has the possibility to receive his/her own personal data or to ask for a direct delivery to the new designated service provider. In the latter case, the Data

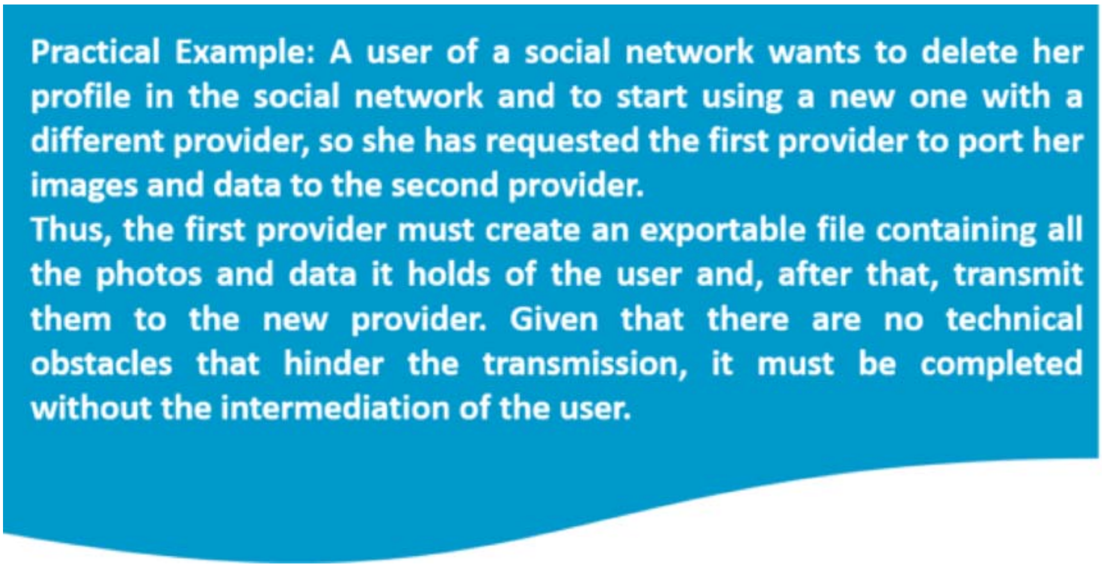
Controller is not required to guarantee the compatibility of its format with the new provider's format, although the GDPR does state that providers should be encouraged to use compatible formats.

Portability is limited to the data subject's personal data only, so the generation of the data cannot prejudice the rights of other data subjects.

What to do to adapt?

Every Data Controller must erase the personal data of any data subject upon his/her request provided that there is no legal ground that legitimizes its processing. To facilitate the response, Data Controllers should establish appropriate protocols to analyze the request and, where appropriate, to grant the erasure. In addition, if the personal data has been made public by the Data Controller, it shall establish measures, including technical measures, designed to inform other Data Controllers who are processing such data to erase any link or copy of the data.

With regards to the right to data portability, the Data Controller must ensure it is capable of delivering the personal data to the data subject (or the new service provider at the request of the data subject) in a structured, commonly used and machine-readable format. Data Controllers shall also facilitate the data request, where possible, in a format that is compatible with other systems. They must also establish technical measures to prevent the generation of such structured files to include personal information of other data subjects.



Practical Example: A user of a social network wants to delete her profile in the social network and to start using a new one with a different provider, so she has requested the first provider to port her images and data to the second provider.

Thus, the first provider must create an exportable file containing all the photos and data it holds of the user and, after that, transmit them to the new provider. Given that there are no technical obstacles that hinder the transmission, it must be completed without the intermediation of the user.

Practical Example: A user of a social network wants to delete her profile in the social network and to start using a new one with a different provider, so she has requested the first provider to port her images and data to the second provider.

Thus, the first provider must create an exportable file containing all the photos and data it holds of the user and, after that, transmit them to the new provider. Given that there are no technical obstacles that hinder the transmission, it must be completed without the intermediation of the user.

TEAM

Joaquin Muñoz Rodríguez (Spain)
Pablo Uslé Presmanes (Spain)

Ana Rocha (Portugal)
Ana Festas Henriques (Portugal)

Derek Stinson (UK)
Paula Enríquez (UK)

Read more:

about us

Share on:

Subscribe:

our Newsletters

Contact us:

Website | LinkedIn

Rua Vitor Cordon Nº 10A, 4º piso - 1249 - 202 Lisboa | Portugal
Tel. (+351) 213 223 590 / Fax (+351) 213 223 599

Rua Pedro Homem de Melo, n.º 55, 8º piso - 4150 - 599 Porto | Portugal
Tel. (+351) 223 190 888 / Fax (+351) 220 924 945

-

PORTUGAL / SPAIN / U.K / BOLIVIA / / BRAZIL / CHILE / CHINA / COLOMBIA

USA / ITALY / MEXICO / PERU / VENEZUELA

This article is provided for information purposes only and does not constitute legal advice. Professional legal advice should be obtained before taking or refraining from any action as a result of the contents of this document. If you have any queries regarding this article, please contact CCA Ontier or ar@cca-ontier.com.