GDPR: The moment of truth?

Emmanuelle Inacio takes a closer look at the 4-letter acronym that has been on everybody's lips lately...

EMMANUELLE INACIO
INSOL Europe Technical Officer

> **IN THE DIGITAL AGE, THE GENERAL DATA PROTECTION REGULATION (GDPR) WAS DESIGNED TO HARMONISE DATA PRIVACY LAWS ACROSS EUROPE**

The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) applies since 25 May 2018[1].

In the digital age, the General Data Protection Regulation (GDPR) was designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organisations across the European Union (EU) approach data privacy.

The key article of the GDPR, is "consent".

Consent remains one of six lawful bases to process personal data, as listed in Article 6 of the GDPR. When initiating activities that involve processing of personal data, a controller must always take time to consider whether consent is the appropriate lawful ground for the envisaged processing or whether another ground should be chosen instead. Controllers that ask for a data subject's consent to use these data shall in principle not be able to rely on the other lawful bases in Article 6.

If obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid basis for processing, rendering the processing activity unlawful.

Definition of Consent

Article 4 (11) of the GDPR defines restrictively "*consent*" of the data subject as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*".

As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid.

To assess whether consent is freely given, Article 7(4) of GDPR plays an important role. Article 7 (4) of GDPR indicates that, *inter alia*, the situation of "*bundling*" consent with acceptance of terms or conditions, or "*tying*" the provision of a contract or a service to a request for consent to process personal data that are not necessary for the performance of that contract or service, is considered highly undesirable. If consent is given in this situation, it is presumed to be not freely given (Recital 43).

The GDPR is clear that consent requires a statement from the data subject or a clear affirmative act which means that it must always be given through an active motion or declaration. It must be obvious that the data subject has consented to the particular processing. A "*clear affirmative act*" means that the data subject must have taken a deliberate action to consent to the particular processing. Recital 32 sets out additional guidance on this. Consent can be collected through a written or (a recorded) oral statement, including by electronic means. "*This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data*". Silence, pre-ticked boxes or inactivity on the part of the data subject, as well as merely proceeding with a service, cannot be regarded as an active indication of choice.

Evidence of consent

In Article 7(1), the GDPR clearly outlines the explicit obligation of the controller to demonstrate a data subject's consent. The burden of proof will be on the controller, according to Article 7(1). But the GDPR does not prescribe exactly how this must be done. Therefore, if the controller is not able to demonstrate that the data subject has consented to processing of his or her personal data, this will render the consent invalid. Similarly, if the evidence of consent is considered insufficient, the consent will not be considered valid, rendering the processing activity unlawful, even if it meets all of the other conditions of validity.

Article 29 of the Directive 95/46/EC established a "Working Party on the Protection of Individuals with regard to the

> CONTROLLERS ARE FREE TO DEVELOP METHODS TO COMPLY WITH THIS PROVISION IN A WAY THAT IS FITTING IN THEIR DAILY OPERATIONS

processing of Personal Data", generally known as the "Article 29 Working Party"[2]. As of 25 May 2018, the Article 29 Working Party ceased to exist and has been replaced by the European Data Protection Board (EDPB)[3], which is composed of representatives from the national data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission (without voting right).

In the same way as the Article 29 Working Party, the EDPB monitors the correct application of the new data protection rules, advise the European Commission on any relevant issue, and give advice and guidance on a variety of topics related to data protection. The novelty of the GDPR is that the EDPB will also issue binding decisions in the case of certain disputes between national data protection authorities, thus fostering the consistent application of data protection rules throughout the EU.

In November 2017, the Article 29 Working Party published "Guidelines on consent under Regulation 2016/679"[4]. These Guidelines provide a thorough analysis of the notion of consent in the GDPR.

Regarding the question of the evidence of consent, according to the Guidelines on consent, controllers are free to develop methods to comply with this provision in a way that is fitting in their daily operations. At the same time, the duty to demonstrate that valid consent has been obtained by a controller, should not in itself lead to excessive amounts of additional data processing. This means that controllers should have enough data to show a link to the processing, but they shouldn't be collecting any more information than necessary.

For instance, the controller may keep a record of consent statements received, so he can show how consent was obtained, when consent was obtained, and the information provided to the data subject at the time shall be demonstrable. The controller shall also be able to show that the data subject was informed, and the controller's workflow met all relevant criteria for a valid consent. For example, in an online context, a controller could retain information on the session in which consent was expressed, together with documentation of the consent workflow at the time of the session, and a copy of the information that was presented to the data subject at that time. It would not be sufficient to merely refer to a correct configuration of the respective website.

Neither the GDPR nor the Guidelines on consent of the Article 29 Working Party published considered the role Blockchain could play in the evidence of consent. Indeed, if the data could be tracked by using Blockchain, which is an incorruptible digital register, this would give evidence of consent. Globally, Blockchain could indeed be a consistent step toward data protection. ■

Footnotes

1 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, no longer in force, repealed by the GDPR: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046
3 https://edpb.europa.eu/
4 Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, WP260, November2017: https://iapp.org/media/pdf/resource_center/wp29_consent-12-12-17.pdf

Share your views!