Editorial: A new era for privacy and data protection in the EU: general data protection regulation

Christina M. Akrivopoulou

Greek Refugee Appeals Authority,
Kanellopoulou Avenue 2, PC 101 77, Athens, Greece
Email: akrivopoulouchristina@gmail.com

The European Union has been a pioneer of privacy and data protection from the nineties. The introduction of Data Protection Directive 95/46/EC has revolutionised data protection safety within the EU and led to the introduction of national data protection authorities within the member states that have guaranteed the rights of the individuals in the most effective and fruitful way. Nevertheless, and since the landscape on data protection and safety has altered immensely over the past years, the EU framework had to change on order to adapt to the new circumstances. After four years of preparation, discussions and debate the GDPR 2016/679 has finally been approved by the European Parliament on 14 April 2016 and will be enforced in 25 May 2018.

The main innovative features of the new GDPR are the following:

1 *Breach notification* is mandatory among the EU state members. More specifically, within 72 hours of a data protection safety breach, the competent data processors are obliged to notify their customers and the data protection controllers on a data breach occurred.

2 *Right to access* for the data protection subject. The data protection subject has the right to obtain from the data controller the necessary conformation on whether his/her personal data have been processed and for which purposes. Additionally, the data controller should provide a copy of the subject's personal data in an electronic format. The enforcement of this right is empowering transparency over the processing of personal data.

3 *The right to be forgotten or right to data erasure*. The right to be forgotten provides the data subject with the right to oblige the data controller to erase his/her personal data and cease their further dissemination or any processing by third parties. The right to be forgotten concerns subjects that withdraw their consent or data that are no longer relevant to the original purposes of processing. The right to be forgotten may be balanced by the data controllers to the public interest on the availability of such data.

4 *The right to data portability*. The data subject has the right to receive any personal data concerning him/her and transfer them to another data controller.

5 *Privacy by design*. Privacy by design is a most powerful tool for an effective personal data protection. Privacy by design obliges for the effective inclusion of data protection and safety from the beginning and designing of data processing systems

Thus, privacy protection is not an addition or a result of data processing but the very basis of any system introduced in this area.

6 *Data minimisation*. A very important principle introduce that obliges controllers to hold and use only the data absolutely necessary for their tasks.

7 *Consent*. The framework for consent has been strengthened. Thus, consent must be clear and in plain language and should be distinguished by other matters.

8 *Withdrawal of consent*. Withdrawal of consent must be considered as equally easy as providing it.

9 *Data protection officers*. The role of data protection officers strengthens the self-regulation of personal data protection. The appointment of a data protection officer is mandatory only for those controllers and processors whose activities require a systematic and regular monitoring of data or large-scale activities and specific categories of data, such as those related to criminal convictions and offences. The data protection officer must have an expert knowledge on data protection, must be provided with the appropriate resources in order to carry out his/her activities, can be a staff member of an external service provider, must not carry out tasks that may be in conflict with his/her role and must report directly to the highest level of management.

10 *Increased territorial scope or extra-territorial applicability*. One of the most crucial elements of the GDPR is its extended jurisdiction to all companies processing personal data of subjects residing in the EU regardless of the company's location in an EU member state or not (clouds are included). This also concerns personal data processing by controllers of processor that do not reside in the EU if the activities relate to offering goods or services to EU citizens and the data monitoring occurs within the EU. These companies are obliged to appoint a representative in the EU if they wish to process personal data of EU citizens.

11 *Penalties*. Companies and organisations that violate the guarantees set out by the GDPR can be fined up to 4% of their annual global turnover or 20 million Euros regarding to which of the two is greater. This is the maximum fine that can be imposed. The fines guarantee the maximum level of compliance to the guarantees set out in the GDPR.

Undoubtedly the new GDPR strengthens the existing former EU legal framework on data protection by adding new and important guarantees regarding data protection safety. Thus, one could say that the burden of data protection is transferred to data processors and controllers that are obliged in designing data protection proofed systems that provide with the maximum protection of the subject's rights. From this point of view is clear that the GDPR aims in the empowerment of the individual in an era where his/her data are more and more endangered by the augmented use of technology. The practical enforcement of the GDPR will surely re-open the discussion on its strengths and weaknesses which remain to be seed.