# ENISA's Position on the General Data Protection Regulation (GDPR)

## 1 Introduction & background

This note briefly summarises ENISA's position on the General Data Protection Regulation. It provides the background to the legislation, explains its significance, provides an overview of the content and discusses the implications for ENISA.

## 2 Background

In 2012, the European Commission put forward its EU Data Protection Reform proposal. On 15/12/2015, an agreement was found with the European Parliament and the Council, following final negotiations between the three institutions (so-called 'trilogue' meetings). The Reform consists of two instruments:

- The General Data Protection Regulation (GDPR), and
- The Data Protection Directive, for the police and criminal justice sector.

Following political agreement reached in trilogue, the final texts will be formally adopted by the European Parliament and Council at the beginning of 2016 and the new rules will become applicable two years thereafter. During this transition phase of two years the Commission will work closely with Member State Data protection authorities (DPA) to ensure a uniform application of the new rules. At the same time the EC will inform citizens about their rights and companies about their obligations.

## 3 Significance

The General Data Protection Regulation is expected to enable people to better control their personal data. At the same time modernised and unified rules will allow businesses to make the most of the opportunities of the Digital Single Market (DSM) also benefiting from reinforced consumer trust.

## 4 Overview of Content

The main points of the GDPR can be summarised as follows:

- easier access to users own data;
- a right to data portability for easier transfer of personal data between service providers;
- a clarified "right to be forgotten";
- the right to know when a user's data has been hacked;
- one-stop-shop with one single supervisory authority;
- companies based outside of Europe will have to apply the same rules when offering services in the EU;
- data protection safeguards are built into products and services from the earliest stage of development (Data protection by design).

# 5 Implications for ENISA

ENISA welcomes the GDPR as an important step forward for enhancing privacy of EU citizens, harmonizing data protection rules across Member States, and promoting privacy and security as core aspects of the European industry. ENISA has already produced and will continue to provide valuable contributions that support the proper implementation of crucial aspects of the GDPR, such as

- the concepts of privacy and data protection by design,
- the practical implementation of the new user rights,
- technical solutions for transparency and user control in digital environments, and
- data breach notification management, risk assessments and security measures for the protection of personal data.

*Privacy and data protection by design*

Among the new elements of the GDPR is the introduction of the data protection by design concept to online and mobile services, which can be performed through the deployment and further use of specific privacy enhancing technologies (PETs) at the various phases of the processing of personal data. This new approach can be beneficial both for the individuals/end users, as well as the EU industry who, by building on PETs, can promote privacy as a competitive advantage.

ENISA has been exploring the role and potential of PETs for several years. Hence, we are in an excellent position to support all involved stakeholders in making the right decisions (end users, industry, as well as DPAs in their advisory/regulatory role). Related ENISA work in the field includes: Privacy and data protection by design[1], Readiness analysis for the adoption and evolution of PETs[2], Privacy by design in big data[3], Online privacy tools for the general public[4]. In the next two years ENISA will continue on this topic by developing a methodology for the assessment of PETs for online and mobile users (the PETs control matrix), as well as by working on the evolution and state-of-the-art of PETs and their building blocks in different sectors.

*New user rights, transparency and control*

One very important objective of the GDPR is the empowerment of the end users with regard to the processing of their personal data in digital environments. To this end, a lot of focus will be put on new mechanisms for transparency and user control, including the practical implementation of consent in online and mobile applications. The introduction of the new rights to data erasure (right-to-be-forgotten) and data portability also contributes towards the same goal.

ENISA has already provided work in this field by studying transparency and control mechanisms in big data[5], addressing privacy considerations with regard to online behavioural tracking[6], as well as analysing the

[1] https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design
[2] https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pets
[3] https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/big-data-protection
[4] https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-tools-for-the-general-public
[5] https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/big-data-protection
[6] https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking

practical implementation of the right-to-be-forgotten[7]. In the next years, ENISA will continue its contributions in this field supporting all involved stakeholders (end users, data controllers, DPAs). In this respect, special attention will be given to the concept of personal data management platforms (often referred as Personal Data Clouds or Personal Data Stores), which can put the user in control of his/her personal data when interacting with multiple data controllers. Such systems can be beneficial in online and mobile environments both for the individuals/end users, as well as the data controllers who can move towards more accountable and user-centric data management.

*Security of personal data*

Security had always been central in the protection of personal data. The GDPR is reinforcing this obligation for the data controllers and processors, following a risk-based and impact-driven approach. ENISA has great expertise on this topic and has produced baseline security measures in different sectors and specialised guidance, in particular related to the use of cryptographic techniques[8]. In the next years ENISA will explicitly focus on risk assessment methodologies and security measures for the protection of personal data, targeting especially the data controllers of different scales and sectors and providing relevant guidance and training material. The DPAs will also benefit from this work as they can be supported in their day-to-day activities and decision making with regard to security and personal data protection.

*Reporting on personal data breaches*

Another important element of GDPR is the notification of personal data breaches. In the new framework, this obligation extends to all sectors, going beyond its current applicability to the telecom operators (under the ePrivacy Directive). This new obligation is in fact an accountability measure for the industry who, on one hand needs to take all the necessary security measures to avoid data breaches and on the other hand has to notify these breaches to the competent authorities and to the affected individuals.

ENISA has provided a lot of work in this field[9] in co-operation with DPAs and NRAs. One of the main elements of this work is a tool for online data breach notification reporting and management, which also provides the possibility for assessing the severity of the breaches (based on a specific methodology[10]). This tool will soon be available to any interested DPAs/NRAs, supporting day-to-day management and prioritization of data breach notifications.

# 6 Conclusions

The General Data Protection Regulation is an important step forward for enhancing privacy of EU citizens, harmonizing data protection rules across Member States, and promoting privacy and security as core aspects of the European industry. ENISA is already well positioned in order to provide valuable contributions that support the proper implementation of crucial aspects of the GDPR during the two years transition phase before its application.

[7] https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten
[8] https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/recommended-cryptographic-measures-securing-personal-data
[9] https://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn
[10] https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn-severity