ENISA HAS PUBLISHED ITS REPORT “ONLINE PLATFORM FOR SECURITY OF PERSONAL DATA PROCESSING. REINFORCING TRUST AND SECURITY IN THE AREA OF ELECTRONIC COMMUNICATIONS AND ONLINE SERVICES”.

SERGIO GUIDA

Independent Researcher, Sr.Data/Information Governance Mgr.

Key-words: ENISA cibersicurezza - GDPR - online platforms – certification

Category: Technical Area

As known, the mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of security across the Union, by actively supporting the Member States, Union institutions, bodies, offices, and agencies.

‘Appropriate’ security of personal data processing is a key obligation for data controllers and processors under the GDPR Article 32, so ENISA proposed in 2018 a risk-based approach for the adoption of security measures. Notably, risk treatment would need to integrate privacy enhancing technologies, e.g. technologies reducing the identifiability of data subjects (and not necessarily qualifying under the “classic” Confidentiality, Integrity, Availability (CIA) triad - protection technologies). Two broad categories of measures, organisational and technical ones, which are further divided into specific categories, are considered and in principle they follow the categorization given in ISO/IEC 27001:2013 (Annex A) and ISO/IEC 27002:2013. The proposed security measures incorporate also additional controls that are specific to the processing of personal data but do not take into account other additional sector specific security requirements, as well as specific regulatory obligations, arising for example from the ePrivacy Directive or the NIS Directive.

To simplify the process for SMEs, the ENISA’s approach defines four areas of assessment for threat occurrence probability, namely:

- Network and technical resources (hardware and software).
- Processes/procedures related to the data processing operation.
- Different parties and people involved in the processing operation.
- Business sector and scale of the processing.

In order to support the practical implementation of the aforementioned guidance, ENISA decided under its 2019 work programme to provide an online platform, which would consolidate and simplify the risk-based adoption of security measures for all interested parties.

The online platform incorporates practically the different steps for a risk-based approach proposed by ENISA and guides any interested organisation (e.g. a data controller or processor) through an assessment of the level of security risk, leading to a list of proposed security measures appropriate to the risk presented. In addition, the platform provides the possibility of a security self-assessment, i.e. assessing the measures that have been adopted by an organisation in front of the perceived/identified level of risk.

The platform may also be of interest to Data Protection Authorities, as a tool that can support the security of personal data processing.

It should be noted that ENISA's online platform is explicitly focused on the security of personal data processing and does not constitute a Data Protection Impact Assessment (DPIA) tool, which is of broader nature. However, ENISA's platform could be utilised in the context of a DPIA tool, as far as security of personal data processing is concerned.

The structure of the report is as follows:

- Section 2 provides a summary of ENISA's guidelines on the security of personal data processing (which forms the basis of the platform's functionality).
- Section 3 presents the main functionality of the platform, which consists mainly of two parts: a) A security risk-assessment approach for personal data processing; b) A security self-assessment tool for data controllers/processors.
- Section 4 draws some conclusions and recommendations with regard to further steps in the field.
- The online platform is available under https://www.enisa.europa.eu/risk-level-tool/.
- The homepage of the tool displays the four different options that are available to the user:
- Evaluating the level of risk for a personal data processing operation.
- (Self)-assessing implemented security measures.
- Overview of the ENISA's guidelines upon which the risk assessment methodology is based.
- Relevant ENISA studies in the field.

The last step in the online platform is the export in PDF format of all the input that the user provided for the specific processing operation, in addition to the identified level of impact, the threat occurrence probability, the level of risk and the proposed technical and organisational security measures. This export provides to the user (organisation acting as data controller/processor) with the detailed analysis of the performed risk-assessment on the basis of ENISA's guidelines.

Ultimately, the online platform for the security of personal data processing is part of the work of ENISA in the area of privacy and data protection, which focuses on analysing technical solutions for the implementation of GDPR, privacy by design and security of personal data processing.

GDPR in its article 42 provides specific provisions for the certification of data processing operations; the Regulation (EU) 2019/881 (Cybersecurity Act) established a European framework on cybersecurity certification. So, while the two frameworks differ in nature and in scope, they could mutually benefit from a joint approach in the area of security of personal data processing: relevant risk assessment methodologies and tools can greatly contribute towards the definition of relevant synergies in the field.

Indeed, the report stresses how the European Commission, Data Protection Authorities and Competent EU bodies should explore the possible synergies between different certification frameworks as regards the security of personal data processing.

Source: European Union Agency for Cybersecurity (ENISA)

Link: https://www.enisa.europa.eu/news/enisa-news/securing-personal-data-a-risky-business