ENISA – Garante Workshop Notes

Meeting:	Workshop on security of personal data processing
Location:	Rome
Date:	08/02/2018
Website:	https://www.enisa.europa.eu/events/ws_personal_data_processing/

One of the core obligations in GDPR for all businesses, including SMEs, acting as data controllers or data processors, is that of the security of personal data processing. According to GDPR, security equally covers confidentiality, integrity and availability and follows a risk-based approach: the higher the risk, the more rigorous the measures that the controller or the processor needs to take (in order to manage the risk).

Against this background and in the context of relevant ENISA's work in the field, ENISA and the Italian Data Protection Authority - DPA (Garante per la protezione dei dati personali) co-organized a workshop on security of personal data processing in February 8, 2018 in Rome. The scope of the workshop was to discuss existing tools and methodologies, address the state-of-the-art in security measures, as well as examine the readiness of data controllers, and especially SMEs, to adopt security measures for personal data processing.

The workshop was addressed to Data Protection Authorities, data controllers and processors, as well as the research community in the areas of security and privacy.

This document presents in brief the key points made during the workshop and relevant conclusions.

1. Opening

The workshop was opened by Ms. Athena Bourka (ENISA) and Mr. Giuseppe D'Acquisto (Garante) who welcomed the participants and introduced the key topics of the agenda.

2. Security as a principle

Mr. Giuseppe D'Acquisto (Garante) in his introductory speech outlined the role of security as a principle in GDPR (art. 5, 24 and 32). Although risk per se is an abstraction, he argued that risk metrics matter and risk assessment should be performed in an accountable way. Moreover, he emphasised that an engineered risk based approach can save costs and give more safeguards. To this end, methodologies that can provide for an accountable risk-based assessment (and subsequent adoption of security measures) are of upmost importance in the context of GDPR.

3. ENISA guidelines for security of personal data processing

Mr. Prokopios Drogkaris (ENISA) presented ENISA's guidelines for the security of personal data processing[1], which have been developed in co-operation with experts from the Italian and Hellenic DPAs and are especially focused on SMEs. The guidelines comprise of four steps, i.e. a) understanding of the context of the processing, b) evaluation of the impact (to the rights and freedoms of data subjects), c) evaluation of the threat occurrence probability, and d) evaluation of the overall risk. The definition of the risk level follows a traffic-light system, i.e. low risk (green), medium risk (yellow), high risk (red). In order to explain the application of the methodology, Mr. Drogkaris showed an example use case from the relevant ENISA's handbook on security measures for SMEs[2].

Ms. Georgia Panagopoulou (Hellenic DPA) further elaborated on the practical use of ENISA's guidelines and in particular on the analysis of specific use cases. She especially referred to the challenges of evaluating impact (on confidentiality, integrity and availability), as there are always cases where the overall impact could be higher than the proposed one. She also outlined the difficulty to establish generic use case scenarios, as well as the fact that the risk assessment is performed per data processing operation (and not per organisation).

4. National and European risk assessment methodologies for personal data

Mr. Felix Bieker (ULD) presented the German GDPR risk assessment framework, which can be assessed with data protection goals (these are, in addition to the classic IT security protection goals confidentiality, integrity and availability: data minimization, unlinkability, transparency and intervenability). In this context, he highlighted various risk sources (controllers/processors, third parties, adverse events), the possible damages (material and non-material) and also referred to possible tensions between different security measures and data protection goals (e.g. availability and integrity may conflict with data minimization, confidentiality may hinder transparency and intervenability, etc.). The proposed framework is currently under discussion and evaluation in Germany.

Mr. Massimo Attoresi (EDPS) presented the EDPS approach to the accountability requirements for EU institutions on documentation, DPIA and prior consultation. In this context, he explicitly referred to the role of the security risk assessment as part of the data protection impact assessment (DPIA); he also discussed the relation between security risk assessment for personal data and the 'traditional' corporate IT security risk assessment. Last, he addressed the area of personal data breaches and the new obligation of data controllers for notification of breaches to the competent authorities and communication to data subjects.

---

[1] Guidelines for SMEs on the security of personal data processing https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

[2] Handbook on Security of Personal Data Processing https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

The discussion that followed focused mainly on the interplay between the 'traditional' risk assessment and the data protection risk assessment, especially if and how they complement each other and whether conflicts could occur (and how they could be addressed).

5. **Panel discussion: Security of personal data processing – a research perspective**

Moderator: Mr. Fernando Pocas Da Silva, EU-LISA DPO
Speakers: Prof. Giuseppe Francesco Italiano (University of Rome – Tor Vergata), Prof. Alessandro Mantelero (Polytechnic University of Turin).

The panel focused on security in GDPR from a research perspective, in terms of both the state-of-the-art, as well as the legal interpretation of security as a principle.

Prof. Giuseppe Francesco Italiano outlined the notion of functional security, i.e. the fact that security is not only seen as a defence mechanism, but also as a guarantee that systems work properly. To this end, he underlined the importance of privacy and security by design, as well as the lack of relevant culture in many organisations and businesses today. He also emphasised the need for further work in key security technologies, such as homomorphic encryption and secure multiparty computations, especially with regard to practical implementation.

Prof. Alessandro Mantelero referred to key challenges with regard to the implementation of GDPR today. He highlighted the shift from legitimacy and data subjects' self- determination to data controllers' accountability and risk management, which makes practical application (of the data protection rules) and enforcement very important. He also mentioned the fact that there is still a lot of room for self-assessment within GDPR (e.g. DPIA) and expressed the underestimation of the collective dimension of use of personal data. Last, he underlined the need to promote security as a cultural value within businesses and organisations.

6. **Panel discussion: Security of personal data processing – from policy to implementation**

Moderator: Mr. Alessandro Spina, EMA DPO
Speakers: Ms. Paola Redecilla (Experian), Mr. Nicola Orlandi (Novartis Pharma AG), Mr. Fabio Guasconi (European Digital SME Alliance)

The panel examined the practical implementation of GDPR art. 32 by data controllers, with specific focus on SMEs.

Ms. Paola Redecilla explained the challenges introduced by GDPR and the way her company is preparing to meet them. She particularly referred to the notion of risk, the need for collaboration between industries, as well as the need for code of conducts (involving industry, consumers and regulators). She also underlined the fact that GDPR can be perceived as an opportunity and privacy as a competitive advantage for EU companies.

Mr. Nicola Orlandi described privacy in the pharma sector as the balance between individual and societal expectations and interests. To this end, he referred to the need for trust and the ethical dimension of data protection, especially in the sensitive area of health. With regard to

GDPR implementation, he empathised the need on one hand of a clear strategy (by the data controllers) and rules, and on the other the need for clear guidelines and support.

Mr. Fabio Guasconi explained the main challenges that SMEs face (in the area of IT security with consequences on data protection), such as lack if IT security culture and awareness, underestimation of security risks, lack of staff and resources. These challenges make SMEs easy target for cybercriminals and a possible entry point to IT systems of bigger enterprises (supply chain risk). He highlighted the importance of EU-driven initiatives involving HUBs, training and trust marks (with less formalised procedures). To this end, he also presented the guide that the European Digital SME Alliance published for the practical implementation of ISO/IEC 27001:2013 for SMEs.

7. Conclusions

The workshop addressed a broad range of topics for security under GDPR, from legal and technical perspective. Some of the main findings and/or open questions are as follows:

- Security as a principle

  Article 5 of the GDPR gives a very prominent role to security: it is in fact a new principle, a necessary prerequisite for the processing of personal data. How to foster a "security culture" among controllers that brings security to the level of a principle is one of the main challenges of the GDPR. To this goal, more reflections are needed from the regulatory community, as well as from the industry, on new security paradigms (e.g. "functional security") that go beyond traditional "defensive security", and that could be more widely and effectively adopted by data controllers.

- Security risk assessment and data protection impact assessment in GDPR

  Security risk assessment (art. 32 GDPR) is based on the evaluation of impact for the rights and freedoms of data subjects. Therefore, it is closely linked to the data protection impact assessment (art. 35). However, while security risk assessment is required for all data controllers (art. 32), data protection impact assessment is not always mandatory. Could this trigger the need for a preliminary data protection impact assessment (including security risk assessment) to be carried out in all cases of personal data processing? Further guidance is needed on the interplay between the two processes, as well as the relevant obligations of data controllers.

- Security risk assessment for personal data and 'traditional' risk assessment frameworks

  Security risk assessment under GDPR needs to fit into the 'traditional' risk assessment frameworks of organisations and businesses. However, combing the two processes is not always easy; in some cases, the two processes might even end up in contradictory requirements. Can security under GDPR be considered as an additional requirement under the 'traditional' risk assessment frameworks? What could the role of privacy standards be to that end? Further work needs to be done in this field, so as to provide more guidance to controllers and especially SMEs.

- Defining the ‘state-of-the-art’

  According to art. 32 GDPR, the data controller/processor should adopt measures based on the ‘state-of-the-art’. However, it is not always clear what is the ‘state-of-the-art’; most existing methodologies point to broad categories of measures rather than specific technologies. It is, thus, important to work towards a more detailed analysis of standards/tools/technologies that could support such an exercise.

- Security measures and PETs

  What is the interplay between article 32 (security) and article 25 (data protection by design and by default) GDPR? This interplay needs to be further explored, also in the light of data protection principles (e.g. data minimization), and of the other provisions and new definitions of the GDPR (e.g. pseudonymization), both when considering risk assessment methodologies, as well as in the analysis of the state-of-the-art for security measures.