ENISA Workshop on Security of Personal Data Processing

Meeting:	Workshop on security of personal data processing Organized in co-operation with the European Digital SME Alliance and the support of the Hellenic Data Protection Authority.
Location:	Athens
Date:	October 8th 2018
Website:	https://www.enisa.europa.eu/events/personal-data-security/personal-data-security

One of the core obligations in GDPR for all undertakings, including SMEs, acting as data controllers or data processors, is that of the security of personal data processing. Appropriate security of the personal data has been elevated in one of the GDPR's principles. The Regulation follows the classical CIA triad approach, so the primary focus of information (personal data in that case) security is on the balanced protection of confidentiality, integrity and availability, along with resilience which is explicitly added in the security related articles, recognizing the importance of high availability for the digital world. As with the previous legislation a risk-based approach is followed but a new set or risks, data protection risks, is defined.

Against this background and in the context of relevant ENISA's work in the field, ENISA with the support of the European Digital SME Alliance, and the Hellenic Data Protection Authority organized a workshop on security of personal data processing, in October 8, 2018 in Athens. The scope of the workshop was to discuss SMEs preparation for the GDPR, especially with regard to data protection security measures, data protection by design, as well as the new –security related- provisions on data breach notification.

The workshop was mainly addressed to undertakings acting as data controllers and processors, especially on SMEs, as well as to 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.

Welcome Messages

ENISA's Andreas Mitrakas welcomed the participants and introduced Konstantinos Menoudakos, the president of the Hellenic Data Protection Authority, who gave the welcome speech.

Mr. Menoudakos, after congratulating ENISA for promoting a culture of digital security, characterized the first months after the GDPR came into force as a new age for digital rights and responsibilities. Incidents like the recent Facebook data breach, which Mr. Menoudakos named as "the first big GDPR case", indicate that security is an even more important aspect of data protection. The GDPR reaffirms and emphasizes the principles of Data Security and Accountability. Thus, companies, including SME's, have now the chance to put their business in order, in their way to GDPR compliance, and should consider the obligation to develop privacy friendly products as a business opportunity and invest in transparency and trust.

During his salutation, Mr. Mitrakas explained that ENISA's activities include practical advice on privacy protection tools and on the concept of Privacy by Design, as well as on the role of CSIRTs and networks of CSIRTs in cyber security, a necessary structure to ensure a secure and resilient digital environment. The GDPR enhances the principles of the Data Protection Directive 95/46/EC by adding not only the principle of accountability, but also the principle of "integrity and confidentiality". Enhanced provisions on the security of processing are provided in art. 32 of the Regulation. Mr. Mitrakas noted that the role of SMEs in today's EU digital economy is crucial, since more than 80% of EU undertakings are SMEs. The business impact of good and practical legislation is not restricted only to EU but may influence the whole world, even the US.

Panel Session I - SMEs preparation for GDPR

Chair: V. Zorkadis (HDPA director)

Panelists: G. Sabatini (European DIGITAL SME Alliance Project Manager), P. Balboni (ICT Legal Consulting, Cyberwatching.eu), A. Oikonomopoulos (Skroutz S.A.)

Vasilios Zorkadis, presenting the panelists, stressed that the GDPR, in article 30 para 5, already provides for SMEs a derogation for the records of processing activities. In the Regulation's text there are tools that fit SME's needs and facilitate compliance, like Codes of Conduct (art. 40-41), Certifications (art. 42) and the development of sector-specific DPIA frameworks.

Guido Sabatini introduced the European DIGITAL SME Alliance, the largest network of ICT SMEs in the continent. He presented the main pillars of the Alliance's operation that primarily focus on policy issues that are favorable for SMEs. To achieve their goals research and innovation are important, thus the Alliance is involved in several EU funded projects. He made a special reference to the Cyberwatching project on cybersecurity and privacy. An important aspect for SMEs is also helping ensuring access to standardization in a practical and easy format. Finally, SMEs need access to training resources and activities, taking into account the diverse ecosystem of their operation. An important remark made by Mr. Sabatini was that for SMEs there is no "one size fits all" digital solution for security and privacy.

Paoli Balboni followed with a presentation of a simplified approach to the new data protection compliance framework. Presenting the Regulation as a traditional compliance circle, he emphasized on the accountability and data protection by design and by default principles and on the role of Data Protection Impact Assessment (DPIA) as the privacy risk based methodology, since the GDPR follows, in its whole, a similar approach. He explained that every data controller, SMEs included, need to take into account risks on the rights and freedoms of the individuals (and not risks on the enterprise's assets), map these risks and then identify proper security measures to mitigate them. He pointed out that in that risk based approach almost 50% of GDPR compliance controls are digital security related, thus the role of IT personnel in GDPR compliance is important. For SMEs, one of the main "threats" is the provision on data breach notification and communication that can result not only in a fine, but mainly in loss of reputation and clientele. In that sense, he characterized the information notice, which many consultants see as the main step for compliance, as just the tip of the iceberg of compliance. Mr. Balboni proceeded elaborating on how SMEs can face the challenge of the GDPR. He proposed a step by step procedure, where the first step is the proper creation of the record of processing activities (art. 30 of the GDPR), followed by an impact assessment and the selection of proper security measures, including handling of personal data breaches. For these steps he noted that there are available software tools and handbooks that can assist data controllers. SMEs need then to take care of the transparency obligations, in order to provide information to data subjects after choosing the correct legal basis for each activity and finally ensure that data subjects are informed about their rights and how to freely exercise them. Mr. Babloni finally stressed the importance of Codes of Conduct and Certifications for SMEs.

Apollon Oikonomopoulos, Director of Engineering at Skroutz S.A., presented the approach that his company followed in order to comply with the GDPR. He briefly presented their business profile explaining that, before the Regulation, they considered that their operations were built on the principles of "security by design" and "security in depth". So, their first objective was to identify what needed to be done, in order to embed privacy and data protection in their day-to-day processes, from design to development to operations. Their decision was that they needed: records of processing activities, an update of internal policies, a new public Privacy Policy in plain language, determination of the legal bases for processing and to prepare Impact Assessment templates and instructions on when to use them. Skroutz S.A. considered GDPR compliance as a project. It took the work of a dedicated team, consisted of a senior engineer and a lawyer, and a strenuous 3-month effort. A key aspect of their work was how to disseminate information throughout the company, making all the changes persistent and raising awareness in every tier. They not only informed, but aided teams in conducting DPIAs and also performed privacy audits in retrospect for the existing systems, resulting to changes. For the legal part, Mr. Oikonopoulos stressed that their key decision was to rely less on consent as a legal basis and use mainly the legitimate interest with the right to object. He also mentioned that although mainstream media helped raise general awareness on the regulation, the information provided to the public was not always accurate and could be considered misleading, especially on the notion and application of consent. As for the technical measures, they had to remove or mask (hide) personal data from their systems, in cases where data were not necessary. They decided to remove third-party Javascript code that presented possible privacy implications. It was also interesting that, after informing their users of the new policy changes, they noticed a stream of account deletions requests, which they perceived as an opportunity to keep the company's client base clean and more effective. Finally, Mr. Oikonomopoulos focused of the continuing challenges, after the GDPR came into force, namely, the difficulty to find data protection experts, the need to bridge the gap between legal & tech staff, to balance business and compliance, to explore new channels for training and awareness and how to apply privacy by design across the board.

In the discussion that followed the participants posed questions to the panelists. Mr. Oikonomopoulos had the opportunity to elaborate more on the technical measures that Skroutz S.A. had to implement in order to comply with the GDPR. The company had to define retention periods and schedule deletion and anonymization of personal data. They also designed new processes to render data anonymous yet still useful, like aggregating data for statistics.

Mr. Balboni explained that encryption, which is explicitly mentioned in several GDPR provisions, is not a mandatory measure. Data controllers, especially SMEs, need to take into account the cost of encryption and the latency that it can introduce in their procedures, in order to select if and what data are to be encrypted. He also mentioned that one should also take into account that most data breaches originate internally, within an SME and not from an outside attacker. He deduced that privacy must cover all aspects of a company, from down to the infrastructure to up the application and procedures.

With another question, panelists were asked their opinion on the appropriateness of the use of cloud services, especially from a security perspective. P. Balboni said that he might endorse the idea of using a cloud service, but one should carefully consider what the provider is offering in terms of privacy. A. Oikonomopoulos stated that if you can't afford maintaining your own resources or don't want to have your own resources, you should consider cloud services. His company's choice was to invest on their in-house infrastructure. Although cost is one factor, one should consider all factors and risks to make the right choice.

A participant raised the issue of how to deal with cookie provisions, given the diverse, in his opinion, legal framework of the e-Privacy directive and the GDPR, in light of a recent decision by the French Conseil d' Etat[1]

[1] http://www.conseil-etat.fr/fr/arianeweb/CE/decision/2018-06-06/412589

that reaffirmed a decision of the country's DPA (CNIL) that imposed a fine on a website operator for illegal use of cookies. P. Balboni noted that although compliance seems difficult, as the change in consent by the GDPR affects the e-Privacy legislation, there is still much debate in Brussels. His opinion is that a company needs to be conservative, as it is a transitional period. A. Oikonomopoulos stated that in his opinion cookie notices are ineffective and cause fatigue to individuals. He proposed that the issue should be solved with appropriate controls on the browser side, which should be respected by websites

Finally, P. Balboni answered on how easy it is for SMEs to control all flow of information, even down to the infrastructure. Admittedly, this is a difficult task for SMEs that need time and external help. The core of the Regulation is mapping personal data and making sure all operations are designed with privacy in mind. So, the whole ecosystem must adapt to it. Vendors should invest and sell Privacy by Design and that approach needs time to mature. In any case, there is no single solution and a systematic approach needs to be followed.

Panel Session II - Security measures for SMEs

Chair: C. Lambrinoudakis (UniPi)

Panelists: G. D' Acquisto (Garante), P. Drogkaris (ENISA), G. Panagopoulou (HDPA), F. Guasconi (European DIGITAL SME Alliance, SBS)

Giuseppe D' Acquisto opened the second panel, after a short introduction of the panelists by Professor Costas Lambrinoudakis. Mr. D' Acquisto presented the security approach of the GDPR with an example from Italy. The Italian Data Protection Law implementing Directive 95/46/EC was complemented with an Annex containing an exhaustive list of security measures. After the GDPR came into force, Italian legislators, following the Regulation's approach, decided that the old Annex is no longer applicable. In fact, since the EU Regulation is putting security under the principle of accountability, check lists, like those provided in the Annex, are not effective. In the eyes of most SMEs, that created a state of uncertainty. In order to determine the "state of the art" enterprises need to take into account several factors and gather information from many sources. As Mr. D' Acquisto stated, there are some easy sources of information. Data controllers should first be aware of all past events within their domain and other similar data controllers. Data Protection Authorities gather information from all controllers (e.g. through data breach notifications) and usually are notified for new technological advances. Public institutions need to disseminate the knowledge they acquire. An example of that is the guidance documents provided by ENISA, WP29 and currently EDPB. G. D' Acquisto also argued on how SMEs, given a specific budget, can balance the cost of application of security measures achieving the maximum of security goals. He specifically mentioned that SMEs, when negotiating with contractors or vendors need to really start negotiating and not accept what is simply offered. He noted that the GDPR demands a risk based approach, as opposed to a prescriptive approach. Following such an approach SMEs can better allocate their resources and achieve their security goals. Security is no longer defensive, but is now a data protection principle.

Prokopios Drogkaris presented the approach followed in ENISA's guidance documents[2] that aim to support security of personal data processing, especially for SMEs. He explained how the typical risk assessment methodology is applied in cases of data protection risk management, since there are significant differences from traditional security risk management. Calculation of the risks is performed with regards to the rights and freedoms of data subjects. A threat is anything that might result in a personal data breach. Least but not

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

last, when estimating the impact, one needs to take into account the negative effects to data subjects and not to the enterprise. Thus, even secondary effects should be considered. A data protection risk management framework comprises of an assessment of the content and nature of the specific processing, appropriate risk treatment -when data controllers might reconsider the processing operation and consult the DPAs and in some cases come to the conclusion that the whole processing poses risks that cannot be accepted- and also communication of the risks to data subjects to enhance transparency. Mr. Drogkaris briefly presented a 4-step approach that follows a traffic-light system and explained how this approach results in a list of possible security measures, derived from international standards, which provide a simple solution to SMEs for the selection of security measures. His final recommendations were a) that in data protection there can't be no "one-size size-fits" approach, but guidance is needed, b) in order to demonstrate compliance data controllers need a methodology including self-audit and certification and c) SMEs need to communicate data protection principles and the steps they take for compliance to raise awareness.

Georgia Panagopoulou presented the steps taken to deploy ENISA's methodology in practical use cases[3] in order to support in this task SMEs with no data protection expertise or expert (like a DPO). The methodology was applied "horizontally" in a number of typical -for most SMEs- processing operations, deriving from the experience provided by case records of DPAs, like HR records, customer/supplier data for different purposes and access control/CCTVs, but also "vertically" in specific SME sectors like health and education. For the proper calculation of the overall level of risk, an analysis of each processing operation was necessary, based on the methodological steps described earlier. Evaluation of impact on confidentiality, integrity and availability was a challenging exercise, for every use case scenario and under certain circumstances, the overall impact could be higher than the proposed one. Results are highly dependent on the context and environment of each processing activity. So, data controllers must first fully understand themselves their data processing operations, before evaluating the risks. In the cases where DPOs have been appointed, their role is crucial. Ms. Panagopoulou argued that sectorial and global solutions, like the certification schemes, sectorial Codes of Conduct and DPIA templates provided for in the GDPR are appropriate tools for SMEs and can facilitate their compliance.

Fabio Guasconi elaborated especially on the notion of "state of the art" a key concept for deciding on the appropriate security measures, according to art. 32 of the GDPR. He quoted the definition from Oxford dictionary as "The most recent stage in the development [of a product], incorporating the newest ideas and the most up-to-date features" and argued that a good approach could be to investigate security measures frameworks, information security and data protection international standards and guides. Most security measures areas readily emerge to be common among them. In his opinion, there is no all-round single best choice of a framework/standard/guide, since each one can produce adequate results if correctly implemented following an effective risk management process. However, in order to best perform that choice, SMEs should consider factors like regulatory or contractual requirements, stakeholder's preferences, the available competence and readiness of the SME, any business opportunity and also the relevant sectorial culture.

In the discussion that followed the participants posed questions to the panelists. An important question was about the connection of DPO certification schemes to the GDPR certifications. As was mentioned, certification provided for in the GDPR, although not in place yet, cover data processing operations by data controllers and processors, taking into account the specific needs of micro, small and medium-sized enterprises. It is clear that these certifications are not meant for persons (like DPOs). Elaborating more on GDPR certifications the panelists noted that preexisting certification schemes may exhibit characteristics

[3] https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

that resemble GDPR certifications, but these should be approved again by the appropriate Data Protection Authorities and certification bodies, as defined in GDPR article 43.

Panel Session III - Personal data breaches - what an SME should know/do

Chair: D. Kampouraki (EDPS)

Panelists: K. Limniotis (HDPA), P. Van Eecke (DLA Piper), K. Panagos (Vodafone), G. Patsis (Obrela)

Dina Kampouraki, before presenting the panelists, briefly presented the EU legal framework on personal data breach reporting and the available WP29 guidance documents.

Konstantinos Limniotis presented an analysis of the, newly introduced by the GDPR, obligation for data controllers to handle personal data breaches, notify the competent DPA in case a breach that can result in a risk to the rights and freedoms of data subjects and communicate the breach to individuals where that risk may be high. He explained that controllers need to be alerted and prepared, because when an incident occurs, they need to notify the DPA within 72 hours and communicate to the individuals without undue delay, ideally even before notifying the DPA. Mr. Limniotis briefly presented some examples from WP29 opinion on data breach notification under the GDPR and analyzed the procedure to notify the incidents to the Hellenic DPA. Before concluding, he explained that the DPA, in dealing the notifications filed so far, focus on providing guidance to data controllers especially with regard to communicating the incident to the individuals, in order for them to be able to mitigate the results of the breach. Data controllers should not be "afraid" of the DPAs and their fining powers, reaching out to them for guidance. Finally, he argued that data processors should assist controllers to fulfill their data breach handling obligations and that it is crucial to act promptly to remedy the consequences of a breach and to ensure that a similar incident is unlikely to occur in the future.

Patrick Van Eecke presented his view on how SMEs consider data breaches and data breach reporting legal obligations. To achieve that, he analyzed the "DNA" of SMEs. The focus of an SME is mainly on their core business and it is in their mentality to tackle issues when they arrive and by themselves, without extra guidance, as they consider compliance an unnecessary cost. Most of them are of the opinion that this piece of new legislation is not meant for them and even if they get some GDPR training, practical application and especially of the data breach reporting provisions will be confusing and probably will lead to them doing nothing or over reacting. This may result in a risk of non-compliance, an increased risk for data subjects or in a loss of the SME's reputation. Mr Van Eecke argued that changing the mentality of SMEs is difficult and proposed a) more awareness activities tailored for SMEs, like training tools to educate their employees, b) practical and simple guidelines and self-service tools that can be used by non-experts, like cyber incident guidelines for SMEs and tools to assess the severity of a breach.

Konstantinos Panagos, representing one of the big telecom providers in Greece, first presented his company commitment to protecting personal data. That led to the creation of a new internal code of conduct for their employees, while for external vendors, most of which are SMEs, it led to the introduction on new data processing agreements, to be in line with the GDPR provisions. He pointed out that it was not easy for SMEs to deal with the new Regulation and that data breaches are considered the number one legal risk. It is a high probability and high impact incident that "can close a business" as he stated. In today's world of business there is just one way for companies, including SMEs, to comply. And that is to prepare to handle incidents in advance.

George Patsis was the last speaker of this panel, providing the view on data breach handling from the perspective of a cybersecurity company. He presented statistical data that indicate a paradox: Although spending on cybersecurity increases through the years, the number of cybercrime and associated incidents keeps climbing. Wondering if that shows a failure of the cybersecurity market, he argued that fragmentation,

complexity and the lack of sustainability are major causes of this failure. The continuously evolving technology landscape and the rapidly evolving attack surface makes addressing Cybersecurity a complex issue. To tackle this challenge, enterprises need to manage their exposure to data breaches, by reducing the attack surface, by patching and configuring a secure state covering their whole supply chain. Cyber resilience is necessary to reduce the probability of an attack, to minimize the impact of a breach and to defend against persistent attacks.

In the first of the questions that followed, panelists were asked about fines in the GDPR and especially whether SMEs could benefit from "forum shopping" to find the supervisory authority that imposes the lowest fines, exploiting what seems as a weakness of the GDPR. K. Panagos noted that this is a wrong dilemma, since the rest of the world is moving towards EU privacy rules. P.V.Eecke added that the GDPR provides for consistency in its application throughout EU and the EU DPAs cooperate closely and under the umbrella of the EDPB for a harmonized application of the provisions. This was also confirmed by K. Limniotis who also added that the criteria for the calculation of a fine are the same for all Member States (art. 83 para 2 of the Regulation) and that there is already work in the EDPB to proactively tackle this issue, as a special task force has been created in order to ensure the consistent application of fines. He also noted that in Greece, the same criteria have already been used in several decisions of the HDPA when justifying fines. Elaborating more on fines, following another question, P.V.Eecke stated that in case of controller – processor relationships there are levels of liability. So although liability can be limited through contracts, one should keep a granular perspective.

Finally, panelists were asked their opinion on the use of remote desktop software and if it can be considered GDPR friendly. All panelists agreed that, although there are risks in using RD software, there are ways to securely use it, after closely examining the available software solutions and through proper security controls.

Panel Session IV - Data protection by design for SMEs

Chair: G. Yannopoulos (UoA)

Panelists: A. Bourka (ENISA), K. Limniotis (HDPA), V. Verykios (EAP), Y. Kotsis-Giannarakis (HAMAC)

Georgios Yannopoulos presented the panelists and elaborated on the principles of privacy by design and by default. His presentation started from the Regulation's text, reaching to the initial approach of privacy by design and its constituent principles as they were introduced more than 20 years ago. According to him, in order to achieve those principles, data controllers need to consider the methods mentioned in the GDPR (pseudonymisation, data minimisation etc.) but it also important to begin by applying proper data mapping and data inventory procedures.

Athena Bourka started the panel's presentations by focusing on what is the notion of "design" in privacy and data protection. Although the concept of data protection by design is now an integral part of the GDPR, its concrete implementation still remains unclear, especially for SMEs lacking the appropriate resources. ENISA's report on privacy and data protection by design[4] and the PETs assessment tool[5] provide valuable guidance. Ms. Bourka formulated the design process in three steps. First, in order to design for privacy, data controllers should learn to think about privacy, by integrating privacy and data protection into their processing operations, considering that this is a strategic change, which does not only affects technical measures, but also organizational measures and – of course – individuals. Second, the design process needs

[4] https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design
[5] https://www.enisa.europa.eu/publications/pets-maturity-tool

careful planning. The eight strategies introduced in ENISAs first paper provide relevant support for SMEs. Finally, it all comes to implementation, choosing the measures appropriate to the risk. Companies should strive for data minimization and select these methods based on state-of-the-art and on what is available to them, since they are not always in a position to control their vendors. For that last stage, SMEs need practical guidance.

Vassilios Verykios presented the privacy related challenges of big data analytics. Big data are currently important for research purposes in several scientific fields, since they can reveal many aspects of the personal lives of individuals. Since legal obligations, like the GDPR, become stricter, in order to preserve the rights and freedoms of those individuals, researchers and SMEs face new challenges. Mr. Verykios elaborated on the differences of the concepts of privacy and anonymity. Privacy relates to what a person keeps to himself/herself while anonymity to what a person can share, without being identified. To achieve anonymity, de-identification processes are very important but also very troublesome, as there are no easy methods for total anonymity. As a final remark he proposed that successful implementation of a business system should follow the holistic approach of the triangle “People / Processes / Technology”.

Konstantinos Limniotis elaborated more on a similar issue as professor Verykios, explaining how pseudonymisation and encryption can be used as data protection mechanisms. In GDPR, a user cannot be considered anonymous when his/her identity is obvious. Depending on the context, especially when dealing with big data, quasi-identifiers can allow a person’s identification. According to the GDPR, account should be taken of all the means reasonably likely to be used –directly or indirectly- to identify natural persons. In the case of pseudonymisation, data should always be considered as personal data, but the method is a safeguard to reduce data protection risks and further ensure the principle of data minimisation and proportionality. Encryption is a different technique, the main instrument to achieve confidentiality. Data are actually unintelligible, unless decrypted. The GDPR explicitly mentions both pseudonymisation and encryption and proposes pseudonymisation as an appropriate measure in the case of processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Mr. Limniotis noted that some currently known pseudonymisation techniques, such as simple hashing of identifiers, do present some pitfalls and in several cases re-identification by third parties can be feasible. Finally he briefly presented the technical solution adopted in the case of Athens public transportation e-ticketing system, where, after the intervention of the Hellenic DPA, engineers had to redesign the system introducing an appropriate hashing procedure for the storage of identification data.

Yiannis Kotsis-Giannarakis of the Hellenic Association of Mobile Application Companies argued that in the current era, business associations need to build synergies. That includes their attitude towards the implementation of the GDPR. He presented a survey, conducted by the association just before the Regulation came into force, that showed that most SMEs in Greece were not adequately aware of the new provisions and only a small proportion of them had been prepared, since most of them consider the cost of implementation as unaffordable. A valuable finding was that most SMEs seek guidance through their lawyers, accountants and professional associations and only just a few through paid consultants and public authorities. His conclusion was that everyone can benefit from synergies with associations.

In the questions that followed the panelists explained that companies need to rethink and change their mentality, although it takes time. Consumers are now more aware about the implications of the processing of personal data and of their data protection rights. So, for SMEs, this is a new environment. The introduction of the principle of accountability in the Regulation is a game changer. SMEs should consider Privacy by Design as a business opportunity.

Closure

Andreas Mitrakas made the final remarks, thanking the participants and pointed out some of the issues raised in the four sessions. Special reference was made to the notion of data protection risks, the interdisciplinary nature of security in data protection, the need for suitable training and the importance of bringing data protection issues to the CEO level.

Conclusions

The workshop covered important aspects of the GDPR provisions on security of processing, from legal and technical perspective, focusing on SMEs. Some of the main findings and/or open questions are as follows:

- Security as a principle

In GDPR security is for the first time prescribed as one of the core data protection principles. To this end, it is essential to develop the appropriate means that can help controllers perceive security as a principle and accordingly integrate it as a key aspect for their data processing operation (i.e. an aspect that is essential to achieve the overall purpose of the processing).

- Need for security frameworks for personal data processing

There is no "one size fits all" solution when trying to apply proper security measures. There is no single best choice of a security framework, since each available framework can produce adequate results if correctly implemented following an effective risk management process and with a risk based approach. Still, it is important to build coherent frameworks that can support SMEs all the way through the process, from risk assessment to the adoption of appropriate technical and organizational measures.

- Need for trained experts

Compliance with the GDPR is a complex task where a significant part (almost 50% of compliance controls) is related to information security. It is difficult to find data protection experts skilled in both the legal and the tech domain. More focus is needed on interdisciplinary training and activities to bridge the gap.

- Tools that can support compliance

Codes of Conduct, Certifications and DPIA templates are important tools for SMEs. SMEs need more practical guidance on these new tools. Synergies with business associations could help dissemination of guidance. The adoption of practical schemes and methodologies can help to this end.

- Guidance on personal data breaches management

Public institutions, including EU DPAs and ENISA, need to disseminate the knowledge they acquire. Data breach reporting is a valuable resource. More work is needed towards practical application of the GDPR provisions, as well as further guidance that can support SMEs to this end. In this context, it is also essential to analyse and provide further guidance on the issues of liability in case of security incidents, e.g. in the controller-processor relationship.

- SMEs guidance and training

SMEs could benefit from awareness activities tailored for them, such as training tools to educate their employees and guidance on how to disseminate information throughout the company and apply the regulation to every aspect of their business, from the management to the infrastructure. Practical and simple guideline texts and self-service tools that can be used by non-experts are also very important, Examples of such possible guidance include cyber incident guidelines for SMEs, tools to assess the severity of a personal data breach, as well as tools to audit, map and make compliant the internal flow of information (self-check).