Strategic Report

Building information security capacity among European citizens and employees

Funded by the Erasmus+ Programme of the European Union

TeBelSi

This document was produced within the scope of the ERASMUS+ Project “Teilzertifizierung im Berufsfeld Informationssicherheit – TeBeiSi”, Project ID: 2018-1-EN02-KA202-005218

Content

List of Figures

List of Tables

1 Introduction

When entering effective in 2018, the GDPR has evoked a drift in the perception and value of personal data among consumers, firms and the society at large. The introduction of binding and sanctionable standards and laws concerning the collection, storage and processing of personal data was supposed to strengthen consumers rights, set boundaries to the exploitation and collection of data and ultimately increase and ensure the right of privacy and personal freedom in the digital age.

Since then, after many public discussions about sense and nonsense as well as dos and don’ts first frictions have been overcome, and the initial wave of attention has flattened. Data protection has become endemic to the work of every organization. Not only are firms required to assign responsibilities for the proper conduct of data protection in their firm, but every employee needs to be aware of potential data protection breaches in their work routine and the following of set-out procedures. Finally, employees themselves have an interest in the protection of their data when entering a work-relationship, which is subsumed under the employee data protection. Employees as the weakest link in the information security strategy of a firms thereby have to receive special attention. Meanwhile large corporations have launched successfully series of educational programs to train awareness of their staff, priorities in SMEs to built up information security and data protection capabilities have remained low in comparison.

Information Security, which in opposition to Data Protection, does not pose a mandatory position or any legally-binding strings to the work of organizations. However, it touches on many aspects of data processing, collection and storage, and thereby requires a broad education and training for responsible personnel. Education and training, especially in the context of know-how protection of a firm, remains a central aspect to increase the safety of SMEs among the EU. In this report, we aim to set out premises and prospects of education and training of information security and data protection competences among the EU and provide recommendations about the further development especially in an SME environment.

2 Data Protection in the partner Countries

2.1 Poland

Name of Institution	Short Description	Website
Urząd Ochrony Danych Osobowych (UODO) (Office for Personal Data Protection)	UODO is the main state body dealing with personal data protection. As part of the tasks assigned by art. 57 GDPR, this body, among others: monitors and enforces the application of the GDPR; disseminates knowledge about risk, regulations, safeguards and rights related to processing in society, as well as understanding these phenomena; advises the national parliament, the government and other institutions and bodies on data protection matters, considers complaints lodged by the data subject or by the entity, organization or association; conducts proceedings regarding the application of the GDPR, issues decisions, and if it is proportionate - determines the amount of administrative fines for violations of the GDPR and imposes them.	https://uodo.gov.pl/
The GovTech centre	The GovTech centre took over some of the responsibilities from the Ministry of Digitalisation, which was liquidated in autumn 2020. The direct recipients of GovTech services are the broadly defined local and central administration, as well as other entities performing public tasks, such as hospitals, schools or transport companies. The recipients of GovTech services are the public sector but also companies.	https://www.gov.pl/web/govtech
Fundacja Panoptykon (The Panoptykon Foundation)	The Panoptykon Foundation monitors surveillance practices. It examines the law in force, legislative proclivities, actions of public authorities and private companies. They follow media and civic reports. They analyse the information gathered, diagnose problems and react. They give their opinion on proposals for new legislation, raise objections to existing laws and their own proposals for change. They point out abuses and negligence.	www.panoptykon.org
Państwowy Instytut Badawczy NASK	NASK - a state research institute supervised by the Chancellery of the Prime Minister. Its mission is to search for and implement solutions serving the development of ICT networks in Poland and the improvement of their effectiveness and security. The Institute conducts scientific research, development works, as well as operational activity for the benefit of the security of Polish civilian cyberspace. Another important element of NASK's activity is the education of users and the promotion of the concept of information society, mainly to protect children and	www.nask.pl

	young people from the threats related to the use of new technologies.	
ZFODO Związek Firm Ochrony Danych Osobwych (Association of Personal Data Protection Companies)	Companies associated in the Association of Personal Data Protection Companies have many years of experience in business consulting in the field of personal data protection. They provide professional services at the highest level to the largest companies in the private sector, as well as local and central government units. They have experience in a wide range of sectors and industries, which allows them to offer their clients individual solutions tailored to their needs. They have many business partners - law firms, IT and marketing consultancies. This allows them to advise their clients comprehensively - not only in the area of data protection, but in the area of their clients' overall business.	www.zfodo.org.pl
Fundacja Wiedza To Bezpieczeństwo (Foundation Knowledge Is Safety)	The Foundation popularizes knowledge in the field of information security. It organizes scientific conferences, helps to solve problems that people face in everyday life, both in private and in business. They conduct social campaigns to raise awareness. In this way we show what dangers are threatened in connection with the unlawful use of our personal data.	https://wtb.org.pl/

Table 1: Stakeholder from Poland.

Among the most common mistakes in connection with the implementation of RODO (Polish equivalent to GDPR) in Polish companies according to the report "10 biggest mistakes in ensuring compliance with RODO" ZFODO mentions most often:

- Misunderstanding the idea of RODO i.e. implementing it only "on paper". As a result, nobody knows and follows its procedures. Lack of implementation may result in sanctions from the supervisory authority.
- Lack of adequate awareness of information security. Conducting risk analysis by unqualified personnel or those with too little experience, resulting in missing or incorrectly conducted analysis. The result is unidentified threats, possibility of data loss, lack of security.
- Inadequate IT area, lack of identified data retention policy or lack of implementation of retention rules in ICT systems. The result can be loss of data or unauthorized access to data, and inability to realize the rights to which the data refers.

In addition, the following were mentioned: incorrect data protection impact assessment, failure to regulate the data entrustment relationship between entities, confusion between the concepts of controller and processor, lack of implementation of the information obligation procedure, lack of coordinator for the implementation of procedures, lack of awareness among employees, lack of a holistic view of the implementation.

The above-mentioned areas are the "main sins", but there are also other aspects of the implementation of the new regulations which proved to be problematic.

For example, the role of the data protection officer is most often underestimated and his position in the organization is low. Often the DPO is a "handpicked" person. The role of the DPO is often underestimated and his position in the organizational structure is low. The DPO is often recruited, does not have appropriate qualifications and has little influence on the decisions made by the top management, his voice is treated only as an advisory one. The report is published in Polish by(ZFODO 2020) ZFODO (2020).

Information on how RODO has been implemented in practice and the scale of breaches and incidents related to personal data protection among Polish companies and institutions is told, among others, in a report prepared by the Association of Data Protection Companies (ZFODO).

The report covered 454 organizations serviced by Companies affiliated with ZFODO in the period May 2019-May 2020. Among those surveyed were organizations and companies from both the private and public sector. The statistics show that an incident (data protection incident) occurs to the average controller statistically 0.65 times per year. This is an insufficient amount to gain the necessary practice in avoiding or managing such incidents, while a mistake in handling even a single incident can have disastrous consequences for the business.

The report shows that nearly 70% of incidents, were not reported to the supervisory authority. According to Article 33(1) of the RODO, one may not report an incident to the supervisory authority if "the breach is unlikely to result in a risk of violation of the rights or freedoms of natural persons". In 70% of cases, the individuals affected by these incidents were not informed. Regardless of reporting the incident to the Regulator, according to Article 34 of the RODO, "If a personal data breach is likely to result in a high risk of infringement of the rights or freedoms of individuals" then we should also inform the affected individuals themselves.

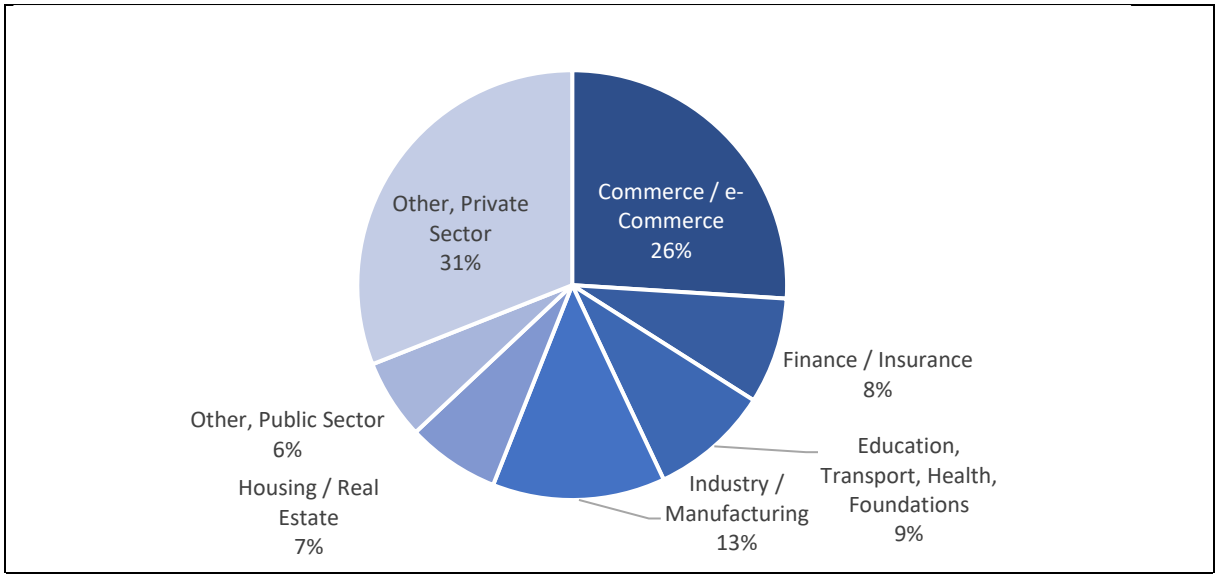

Figure 1: Industries/ branches most at risk of personal data breaches
Source: ZFODO (2021),own illustration.

Source: ZFODO (2021)(ZFODO 2021), own illustration

Sources of personal data breaches were located both inside the company/ institution (68%), outside (20%), as well as came from the so-called processor, i.e. an entity processing data on behalf of the controller (12%). The external ones include, for example, former employees or hackers, the internal ones - employees and associates of the organization.

In 92% of cases these were unintentional (misaddressed e-mails, lack of a hidden copy, sending traditional correspondence with incorrect content). Intentional incidents included: theft of laptops or other data carriers, phishing, sharing data with unauthorized persons. Almost 96% of incidents were caused by personal reasons. These included the action of a human factor. Non-personal causes are situations where the breach was caused by a malfunction of technology, situations beyond the control of human will.

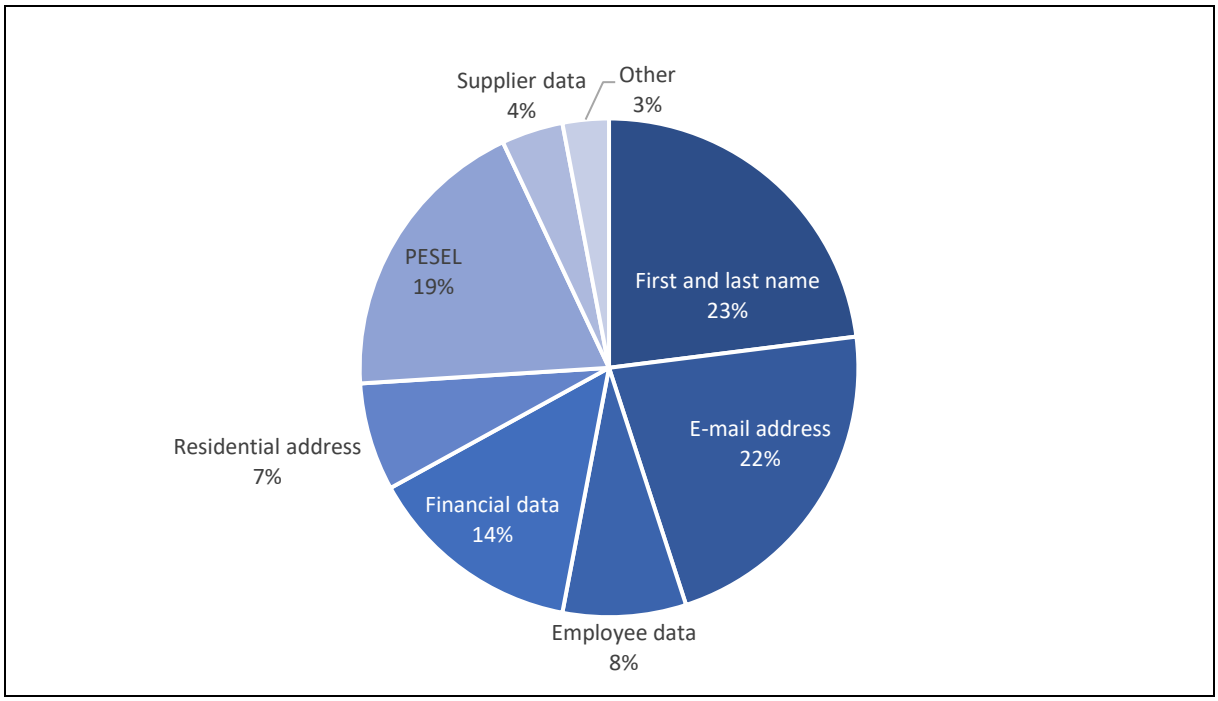

Figure 2: Most frequently breached data categories.
Source: ZFODO (2021)Source: ZFODO (2021),own illustration.(ZFODO 2021), own illustration.

As far as the protection of employees' personal data is concerned, unfortunately no report has been found analysing the scale and the most common situations related to this issue in Poland. In order to facilitate the recruitment process and make it easier to navigate among the regulations, the UODO (Office for Personal Data Protection) has issued a publication entitled "Personal Data Protection at the Workplace. Guidebook for Employers" (Office for Personal Data Protection 2018).

2.2 Austria

Name of Institution	Short Description	Main Purpose	Website
WKO – Austrian Chamber of commerce / WKO Wirtschafts-kammer	The WKO calls on companies to develop an appropriate security strategy that protects against potential threats.	Raising the awareness of employees is an important safety factor. A separate department for IT security and data security has been established. SMEs are supported by various initiatives.	https://www.wko.at/service/innovation-technologie-digitalisierung/it-sicherheit-datensicherheit.html
Austrian Data Protection Authority / Österreichische Datenschutzbehörde (DSB)	The Austrian Data Protection Authority is the national supervisory authority for data protection in the Republic of Austria.	The Legal Information System of the Republic of Austria (www.ris.bka.gv.at) provides Austrian legislation in its current version (federal and state), law gazettes (federal and state) and case law.	www.dsb.gv.at
BFI Wien Training Data Protection and IS	Training provider for Data Protection and IS	As a state-recognized continuing education institute, the BFI is entitled to issue certifications and submit recognition procedures for non-formal training courses to the NQF Coordination Body (NKS) - or via its Service Points.	https://www.bfi.wien/edv-und-informationstechnologien/datenschutz-und-informationssicherheit/
KMU Platform	This network of experts from business and technology was founded to support SMEs in Austria in order to accompany companies in the digital change.	In addition to many other services, workshops on a wide range of topics are offered. The slogan "Common ground replaces size" makes clear that the focus is on cooperation between small companies, which in turn create a competitive advantage for themselves.	https://www.kmu-plattform.eu/
Digitization Agency / Digitalisierungs-agentur	Within the FFG, the Research Promotion Agency, the "Digitization Agency" was set up to award grants to SMEs - small and medium-sized enterprises - in Austria in order to promote digitization in a targeted manner.	In order to enable Austria's small and medium-sized enterprises (SMEs) in particular to make the best possible use of their digitization opportunities, the “KMU DIGITAL Initiative” provides concrete assistance: The companies benefit from subsidies for consulting, qualification, knowledge transfer and further training.	https://www.ffg.at/dia

Vienna Business Agency / Wirtschafts-agentur Wien	The "Wien Digital" funding programme supports MEs and SMEs in implementing digitization measures.	The Vienna Business Agency offers personal consultation and has a broad network of SMEs and (public) cooperation partners. Startups, sole traders, domestic and international small and medium-sized enterprises or corporations are supported in important questions.	https://wirtschaftsagentur.at/
Business Circle	Provider for Training Course for a certified Data Protection Officer	The qualifications acquired in the course are confirmed with the certificate of Austrian Standards according to the criteria of ISO/IEC 17024 after a positively assessed final examination.	https://businesscircle.at/recht-steuern/lehrgang/lehrgang-zum-zertifizierten-datenschutz-beauftragten/
1a Beratung e.U. - Ing. Roland Fürbas	Private Provider for GDPR & IS training courses	Data & IT Security / DSGVO-DSB / Business Development / Online Services	http://www.1a-beratung.eu
72solutions	Private Provider for GDPR & IS training courses	GDPR - Experts who provide advice and develop tailored solutions for data protection measures.	https://www.72solutions.eu
TÜV Austria Akademie	Provider of training courses on data protection - GDPR expert	There are around 20 courses on offer, which are structured according to sector.	https://www.tuv-akademie.at/kursprogramm?s=Datenschutz

Table 2: Stakeholder from Austria

Austria was one of the first European countries with an authority for data protection, the Data Protection Commission. It was created with the first Data Protection Act, Federal Law Gazette No. 565/1978. The EU Data Protection Directive 95/46/EC has put data protection law on a new footing across Europe (EUR-LEX 1995).In Austria, this Directive was implemented by the Data Protection Act 2000 (DSG 2000) (Rechtsinformationssystem des Bundes (RIS) 1999). After 25 May 2018, the Basic Data Protection Regulation (GDPR; DSGVO) has put data protection law on a new footing across Europe EUR-LEX (1995). In Austria, this Directive was implemented by the Data Protection Act 2000 (DSG 2000) Rechtsinformationssystem des Bundes (RIS) (1999). After 25 May 2018, the Basic Data Protection Regulation (GDPR; DSGVO) (Federal Ministry of Finance (BMF)) and the revised Data Protection Act (DSG) (Federal Ministry of Finance (BMF)) form the basis of the data protection law (see DSB 2019).

According to the Austrian Commercial Code (UGB) and the Limited Liability Companies Act (GmbHG), the responsibility for Data protection and IT security always lies with the management. Even if security-relevant IT tasks are handed over to employees, the company management bears ultimate responsibility for compliance with the legal provisions. With the NIS Directive (EU) 2016/1148 (EUR-LEX), which was implemented in Austria at the end of 2018 by the Network and Information

Systems Security Act (NISG), there are for the first time comprehensive regulations in the area of cyber security for strategically important companies, digital service providers and authorities at European and national level. Companies must take appropriate technical and organisational measures (e.g. data backup, encryption, access controls) to protect data from accidental destruction, data loss or unlawful use by third parties. Failure to do so may result in heavy fines.

The EU General Data Protection Regulation (GDPR) and the Austrian Data Protection Act regulate the handling of personal data (e.g. name, date of birth, email address, IP address). This means that all entrepreneurs in Austria are bound by legal regulations. As a rule, companies that have reached a certain level of digitalisation are well acquainted with them and are regularly informed, especially by the Chamber of Commerce. Micro-enterprises, which often place less emphasis on the topics of IS and DP for reasons of time and cost, are more problematic.

The issue of the duty to inform according to GDPR seems to be particularly problematic, which, according to Conrad Lienhardt, is often not applied in Austria, especially in small companies: "According to the General Data Protection Regulation (GDPR), the rights of data subjects, i.e. those whose personal data are processed, include an extensive right to information. On the part of companies and organisations, this means extensive information obligations. These are regulated in Articles 13 and 14 of the GDPR." Lienhardt warns not to underestimate the duty to inform: "There are companies and organisations that obtain personal data from public databases, such as land registers, address directories, etc. and then process it. Many think that they are not subject to the duty to inform, especially since, in addition, "siphoning" data from public directories very often involves large amounts of personal data. Complaints and private actions for damages are to be expected. Therefore: Take the duty to inform seriously." (Lienhardt 2020).

Employee data according to the EU General Data Protection Regulation: In Austria, not only data protection law but also labour and social law provisions apply, as the WKO emphasises: "It should be checked here on what basis data are processed (legal obligation, necessary for the performance of the service contract, consent?). [...] Since the payroll accountant usually acts on the basis of a contract processing relationship with the client (= responsible party) and the client has the obligation to also pay correctly on the basis of the employment relationship, no consent of the respective employee of the client is necessary for this. However, you must conclude a written order processing contract." (Wirtschaftskammer Österreich 2021b).

The WKO (Wirtschaftskammer Österreich), the Austrian Chamber of Commerce, offers also support for the implementation of the GDPR with sector-specific information, guides, sample documents and checklists. The guide on technical and organisational measures in the context of the GDPR provides a practical overview of which technical security measures are necessary and useful and how they can be implemented in the company. (c. f. Wirtschaftskammer Österreich (2020)) Finally, the WKO‘s "IT Safe" (Wirtschaftskammer Österreich 2021a) is a well-established and well-known initiative to support SMEs in implementing IT security measures.

Companies in Austria have numerous sources of information regarding the GDPR at their disposal. However, it is natural that these very extensive legal texts cannot be grasped at a glance. In this regard, the services of the Austrian Federal Economic Chamber should be highlighted, which is an important contact point for all - and especially for small - businesses. With "IT Safe", a comprehensive guide was developed, and numerous free information events are offered. A particularly important offer is a professional website that presents the most important basics of the GDPR in an understandable way (c.f. Wirtschaftskammer Österreich (2021b))

Another attractive offer is made by KSV (Kreditschutzverband), which provides companies with cost-effective support for the introduction of the GDPR on several levels: advice, training and the app "DSVGO Assistant" (KSV1870).

Despite all efforts, people in Austria still like to talk about the "unloved GDPR"! We have found the following - from our point of view - appropriate press release:

The sobering reality in Austrian companies

In this APA (Austrian Press Agency) press release of May 2020, Austrian Press Agency (2020) reports about the implementation of the EU GDPR in Austria under the title: "Understanding yes, implementation sluggish". (Austrian Press Agency) press release of May 2020, Austrian Press Agency (2020) reports about the implementation of the EU GDPR in Austria under the title: "Understanding yes, implementation sluggish".

> "Despite significantly increased sensitivity in matters of data protection, the EU regulation has only been fully implemented by 30% of domestic businesses since 2018."

The article emphasises the fact that two years after the EU General Data Protection Regulation (EU GDPR) came into force, Austrian companies show a significantly increased understanding of the topic of data protection. In a KSV1870 survey, conducted before the Corona crisis, as part of the Austrian Business Check in February 2020 with around 600 companies, 40% of the companies surveyed stated that this had increased "across the board" in the past three years. The survey clearly showed that there is still work to be done before the EU GDPR is fully implemented by all companies in Austria, after only 30% of respondents have fully anchored it in their operations so far. The most frequently implemented measure to increase data protection was named by 46% of the survey participants as the introduction or adaptation of data protection and IT security measures. On a positive note, the author mentions that the understanding for a trusting and conscious handling of information in Austrian companies has increased significantly during the past three years. (Austrian Press Agency 2020) emphasises the fact that two years after the EU General Data Protection Regulation (EU GDPR) came into force, Austrian companies show a significantly increased understanding of the topic of data protection. In a KSV1870 survey, conducted before the Corona crisis, as part of the Austrian Business Check in February

2020 with around 600 companies, 40% of the companies surveyed stated that this had increased "across the board" in the past three years. The survey clearly showed that there is still work to be done before the EU GDPR is fully implemented by all companies in Austria, after only 30% of respondents have fully anchored it in their operations so far. The most frequently implemented measure to increase data protection was named by 46% of the survey participants as the introduction or adaptation of data protection and IT security measures. On a positive note, the author mentions that the understanding for a trusting and conscious handling of information in Austrian companies has increased significantly during the past three years. (Austrian Press Agency 2020)

"Thus, 40 % of domestic companies confirm that this development has taken place "across the board" - another 32 % see an increase at least in partial areas. While for 19% an improvement is not discernible, for 2% it has even decreased." 7% of the interviewees did not give any specification. (Austrian Press Agency , 2020). There is often a considerable gap between understanding and actual implementation of necessary data protection measures. Especially in times of increasing digitalisation due to the Corona crisis, it is particularly worrying that not even a third of domestic companies have fully implemented the EU GDPR," explains Ricardo-José Vybiral, MBA, CEO of KSV1870 Holding AG. This includes, among other things, the required "register of processing operations", which only 34% of the companies surveyed have successfully implemented so far. (Austrian Press Agency 2020).s often a considerable gap between understanding and actual implementation of necessary data protection measures. Especially in times of increasing digitalisation due to the Corona crisis, it is particularly worrying that not even a third of domestic companies have fully implemented the EU GDPR," explains Ricardo-José Vybiral, MBA, CEO of KSV1870 Holding AG. This includes, among other things, the required "register of processing operations", which only 34% of the companies surveyed have successfully implemented so far (Austrian Press Agency 2020).

Deloitte Services Wirtschaftsprüfungs GmbH (2020) also published a study on the degree of implementation of the GDPR in Austrian companies at the beginning of 2020. 191 company representatives in executive positions were surveyed in an online survey: "The result: the majority of companies are still busy implementing the requirements and see their long-term compliance as a challenge. But the importance of the topic has now been recognised: Almost all respondents now take data protection requirements into account when making business decisions." Deloitte Services Wirtschaftsprüfungs GmbH (2020) also published a study on the degree of implementation of the GDPR in Austrian companies at the beginning of 2020. 191 company representatives in executive positions were surveyed in an online survey: "The result: the majority of companies are still busy implementing the requirements and see their long-term compliance as a challenge. But the importance of the topic has now been recognised: Almost all respondents now take data protection requirements into account when making business decisions." Deloitte Services Wirtschaftsprüfungs GmbH ((2020) (2020) also published a study on the degree of implementation of the GDPR in Austrian companies at the beginning of 2020. 191 company representatives

in executive positions were surveyed in an online survey: "The result: the majority of companies are still busy implementing the requirements and see their long-term compliance as a challenge. But the importance of the topic has now been recognised: Almost all respondents now take data protection requirements into account when making business decisions." (Deloitte Services Wirtschaftsprüfungs GmbH 2020)

Similar to KSV, Deloitte also concludes that the full implementation level of the GDPR in Austrian companies is just under one third: "The majority of companies (54 %) are still on the home stretch in implementing the EU GDPR, as they were a year ago. While almost a third (32%) of respondents have now fully completed the implementation of the directive, around 12% are still in the middle of the process and have an acute need to catch up." Deloitte states in the report that there should no longer be any excuses for not having implemented the directive. It is urgently recommended that the companies concerned actively address this issue and, if necessary, seek external help to speed up implementation.

When asked about the implementation status of the GDPR, the companies responded as follows:

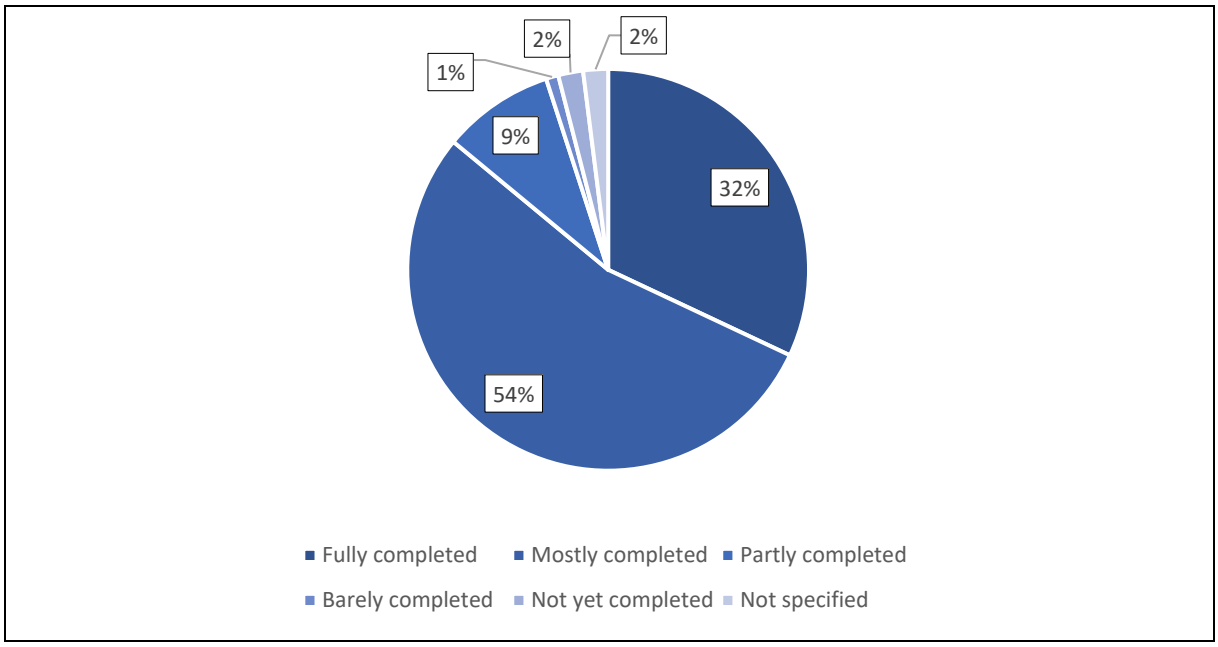

Figure 3: Implementation of GDPR in Austria

Source: Own Illustration. Data used from Deloitte Services Wirtschaftsprüfungs GmbH (2020)

In 2020, as was reported in the media, there was an increase in fines for non-compliance with data protection regulations. Deloitte therefore asked the companies how these notifications influenced the behaviour in the company: "Only in a quarter of the companies have the decisions of the data protection authority had an influence on the handling of the EU GDPR so far. Of these, the majority have used the findings to evaluate or improve the status in their own company." The question was worded as follows: Have the recent decisions of the Austrian data protection authority influenced your approach to the EU GDPR?

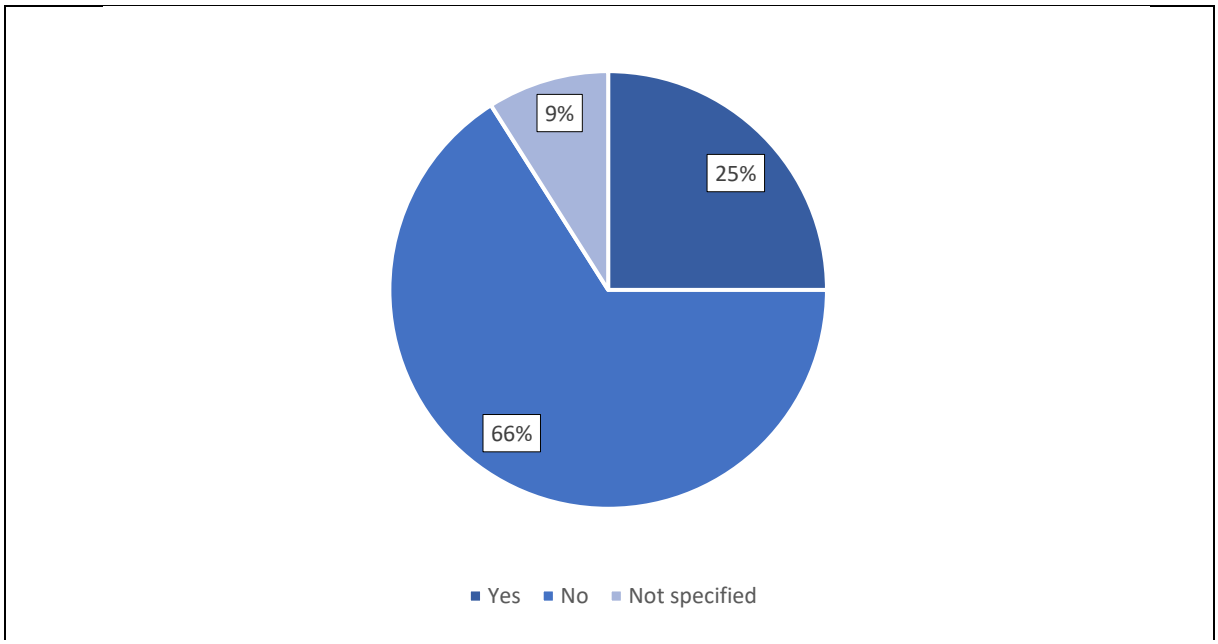

Figure 4: Influence of the Austrian data protection authority on the approach to the EU GDPR

Source: Own Illustration. Data used from Deloitte Services Wirtschaftsprüfungs GmbH (2020)

The Deloitte study emphasises that many companies in Austria have unfortunately failed to do their homework in recent years. There is often a lack of structured data classification, which would significantly reduce the effort. The following evaluation of the next question is interesting: How much effort do you estimate it will take to comply with the requirements of the EU GDPR in the future?

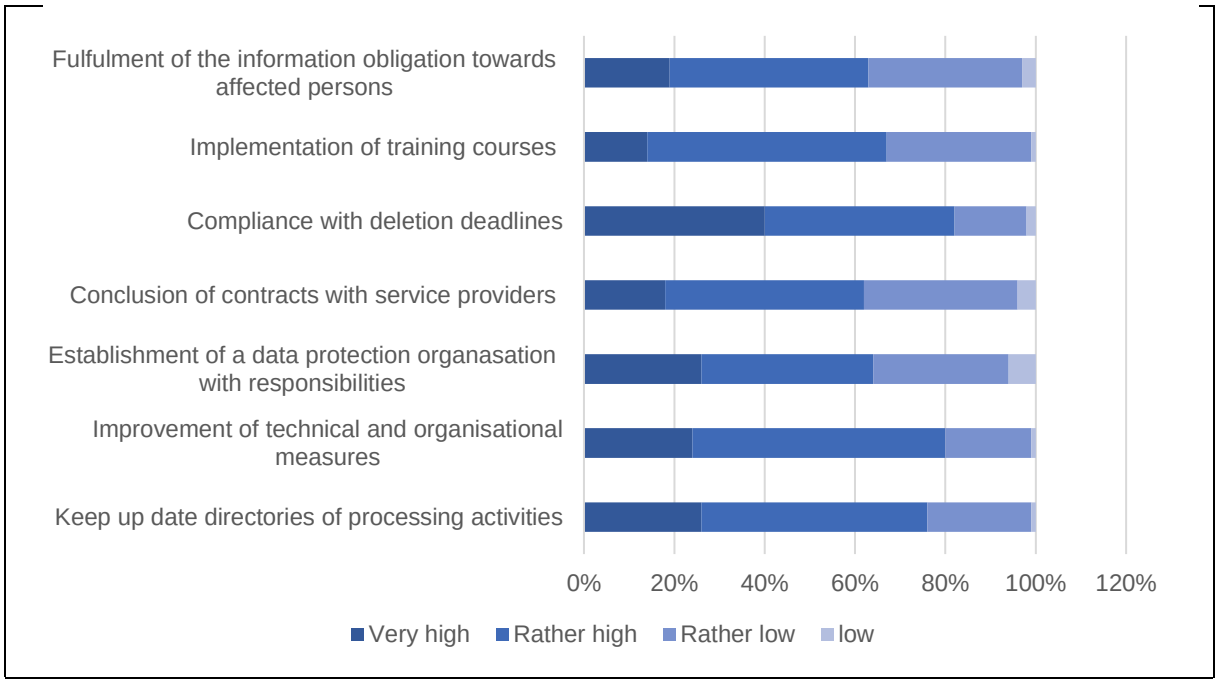

Figure 5: Efforts potentially spend to comply with the requirements of the EU GDPR

Source: Own Illustration. Data used from Deloitte Services Wirtschaftsprüfungs GmbH (2020)

The report shows that for the majority of companies, long-term compliance with the GDPR is experienced as challenging. The respondents perceive the greatest effort in considering deletion deadlines.

Another interesting question by Deloitte is whether there are enough trained employees for data protection tasks: "More than a quarter of the companies surveyed lack the human resources to comply with the EU GDPR and implement the related work. This makes other support all the more important: Thus, more and more Austrian companies are turning to technological support in order to be able to meet the EU GDPR requirements. While 39% did not have a tool last year, it is currently around 30%."

The Deloitte report concludes: "After initial uncertainties, Austrian companies have a much clearer picture of the existing need for action. However, some of the identified key topics involve comprehensive changes. The corporate culture is also affected." Deloitte Services Wirtschaftsprüfungs GmbH (2020)The Deloitte report concludes: "After initial uncertainties, Austrian companies have a much clearer picture of the existing need for action. However, some of the identified key topics involve comprehensive changes. The corporate culture is also affected." (Deloitte Services Wirtschaftsprüfungs GmbH 2020)

From Hafelekar's point of view we can summarise the situation in Austria as follows: It can be said that there are clear laws in Austria on the topic of implementing the GDPR, even though they are not always formulated in a way that is easy to understand. There are several public bodies, first and foremost the WKO, which companies can turn to for support in implementing the GDPR. In Austria, the liability for all misconduct with regard to data protection and IT security lies with the management, even if they delegate tasks to employees. The implementation is still not running satisfactorily and as we have already established with our expert group in Austria, the lack of time in SMEs is probably decisive for this slow implementation. In any case, according to our TeBeISi Steering Group, there is a great interest in Austria for affordable further training on the topics of data protection and IT security. There is still a lot of work to be done.[SR2]

2.3 Germany

Name of Institution	Short Description	Main Purpose	Website
Deutsche Vereinigung für Datenschutz e.V. (DVD)	The DVD is responsible for publishing messages regarding data protection (DANA). Public relations and media work on current topics, press conferences and press releases are also part of the tasks. Besides, meetings in cooperation with partner organizations and seminars are held. The DVD also participates in the annual Big Brother Awards.	The DVD aims to advise and inform the public about the risks of using electronic data processing and the possible restriction of the right to informational self-determination.	https://www.datenschutzverein.de
Gesellschaft für Datenschutz und Datensicherheit (GDD)	Founded in 1977, the GDD has more than 3,800 members today. There are 34 circles for exchanging new experiences nationwide with more than 3,500 participants and more than 10,000 data protection officers have been already trained at the GDD academy.	Data protection, data security and proper data processing are intended to protect all stakeholders from danger while ensuring freedom of information and information balance. Legal obligations affect all companies and administrative units, regardless of size or industry. The GDD wants to make a major contribution.	https://www.gdd.de/
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfG)	About 700 persons from science and practice work at the FIfG, especially professionals in computer science and information technology. The aim is to enable an exchange among all those involved in computer science and information technology. The FiFG is open to all who would like to participate or just want to inform themselves.	FiFG warns the public about harmful developments in the field of information security. Besides, the association fights against the use of information technology for control and surveillance. FiFG also supports equal rights for people with disabilities in the design and use of information technology and works to combat discrimination against women in computer science.	https://www.fiff.de/
Digitalcourage e.V.	The association was founded in 1987. Among others, *Digitalcourage e.V.* supports fundamental rights and data pro-	A major part of the work consists of organizing projects and campaigns but also the organization of political congresses. Further, the association is available to press and media as speakers and experts on data	https://digitalcourage.de/

	tection, provides educational work through public relations, e.g. through campaigns and projects, and is responsible for the annual award of the BigBrotherAward.	protection issues. The main aim is to engage in fundamental rights, data protection and a world worth living in the digital age.	
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDi)	The main tasks of the institution founded in 1978 are monitoring and enforcement of the GDPR, the BDSG and other regulations on data protection. Furthermore, it is about raising awareness and public relations.	The main aim is the safeguarding and development of data protection. Since 2006, anyone who considers their right to access information under the Freedom of Information Act (IFG) to have been violated can contact the Federal Commissioner. The office is currently held by Prof. Ulrich Kelber.	https://www.bfdi.bund.de/

Table 3: Stakeholders from Germany.

The European General Data Protection Regulation (GDPR) came into force on May 24, 2016. As of May 25, 2018, the data protection requirements contained herein are mandatory in the respective member states even without separate transposition into national law. The European data protection regulation is intended to strengthen consumer rights in particular. Data processing agencies have to expect stricter regulations. Non-compliance with the GDPR can cost the company in question up to 20 million euros in fines or up to 4% of its global sales (depending on which value is higher) (datenschutz 2021). The status of implementation of the GDPR by companies in Germany is shown in Figure 3. The statistic was published in autumn last year. It is the most recent study available regarding the implementation of the GDPR. At the time of the survey, 37% of the respondents indicated that they have already implemented the GDPR guidelines. More than half of the participants stated that the guideline is either partially implemented or completely implemented and established for further development (Statista 2020).The European General Data Protection Regulation (GDPR) came into force on May 24, 2016. As of May 25, 2018, the data protection requirements contained herein are mandatory in the respective member states even without separate transposition into national law. The European data protection regulation is intended to strengthen consumer rights in particular. Data processing agencies have to expect stricter regulations. Non-compliance with the GDPR can cost the company in question up to 20 million euros in fines or up to 4% of its global sales (depending on which value is higher) Datenschutz (2021). The status of implementation of the GDPR by companies in Germany is shown in Figure 3. The statistic was published in autumn last year. It is the most recent study available regarding the implementation of the GDPR. At the time of the survey, 37% of the respondents indicated that they have already implemented the GDPR guidelines. More than half of the participants stated that the guideline is either partially implemented or completely implemented and established for further development Statista (2020). [1]

[1] More information concerning the study: Date of publication 09/2020, Germany, survey period 09/2020, number of respondents: 504 companies with 20 or more employees, telephone survey.

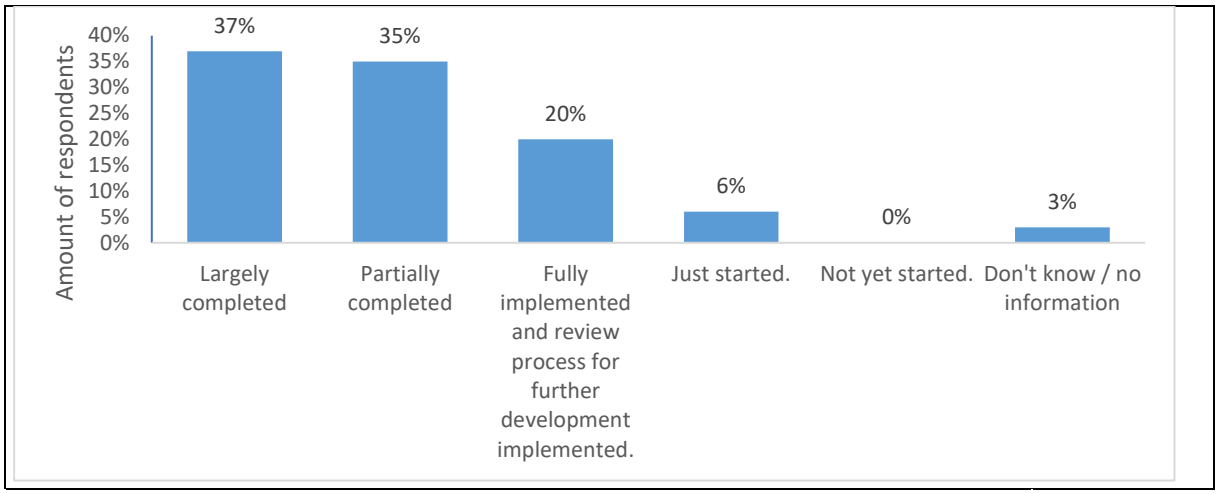

Figure 6: Status of implementation of the GDPR by companies in Germany (09/2020)

Considering the passing of around 5 years of publishing and 3 years acting into force, it can be inferred that severe obstacles prevent firms from fully implementing the GDPR. The specific ramifications have been detailed in the study conducted by Bitkom e.V. (2020). One of the reasons firms struggle with the implementation can be attributed to the large amount of effort needed, starting with an initial (and singular) extra expense (63%), the expectation of a permanent extra expense (compared to the prior legal status, 29%) and the need for extra personnel (26%). The personnel need is also reflected in the decision of firms to buy the service data protection from service providers, either in the form of external legal counselling (40%), external data protection counselling (31%) or external reviews (28%). Nonetheless, the GDPR is perceived by the majority of firms to positively contribute to the operation and the performance of the firm. Considering the effect on uniform competitive environments across the EU (57%).

In the face of complex regulatory changes, however, several aspects spark doubts concerning the positive effect on economic activity. Among others, concerns regarding the long-term improvement if the legal environment (43%), the hampering of innovation (35%) and the complication of business processes (25%) become prevalent. The risks of implementing the GDPR also reflect in the measures which receive the most urgency, as can be seen in Figure 7.

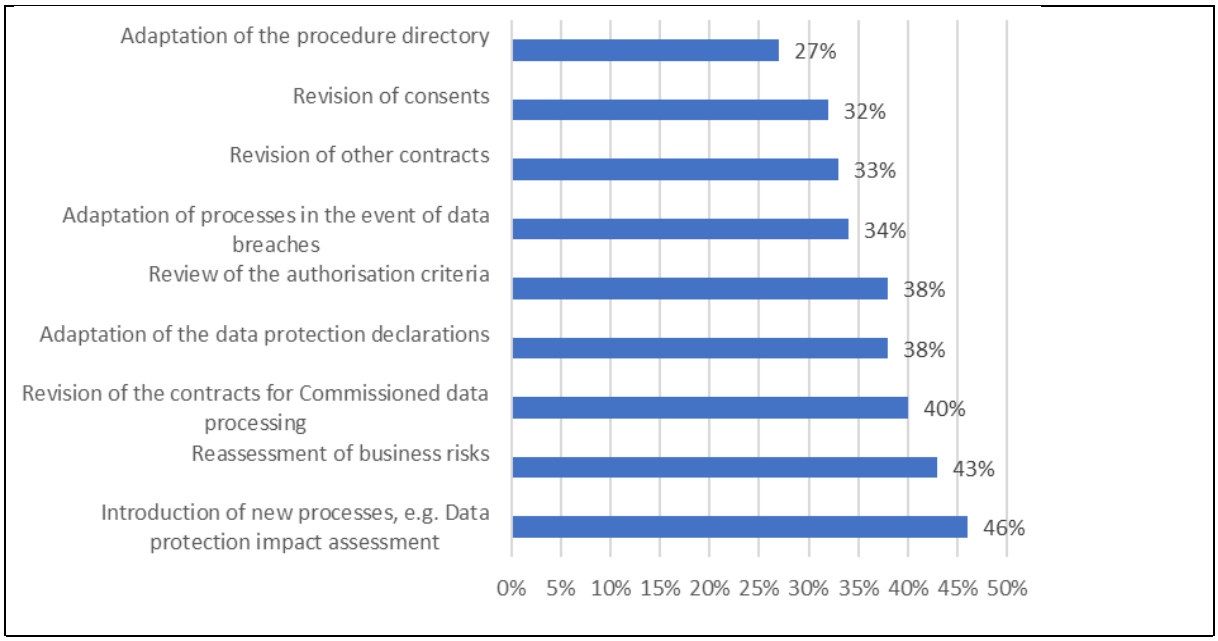

Figure 7: Which measures for the implementation of the GDPR will you implement with high urgency? Source: Bitkom e.V. (2020)

A study conducted in 2021 highlights a generally high prioritization of data protection in Germany, ranking it second among all European countries in the general and appropriate treatment of data protection (heyData 2021). From all categories considered, it is noteworthy that “companies” rank lowest in comparison to “law enforcement”, “data protection competence” and “public sentiment”, and “private individuals” ranking comparatively highest. Each category can be decomposed into several criteria, which shed light onto specific strength and weaknesses. Looking into the situation of firms, as can be seen in Figure 8, it becomes evident that only 17% of firms have mandatory further training in place in comparison to the 24,29% of the EU average. A second major shortcoming in comparison to the remaining EU becomes evident in terms of insurance protection, where Germany scores 4 ppt lower than the EU average.

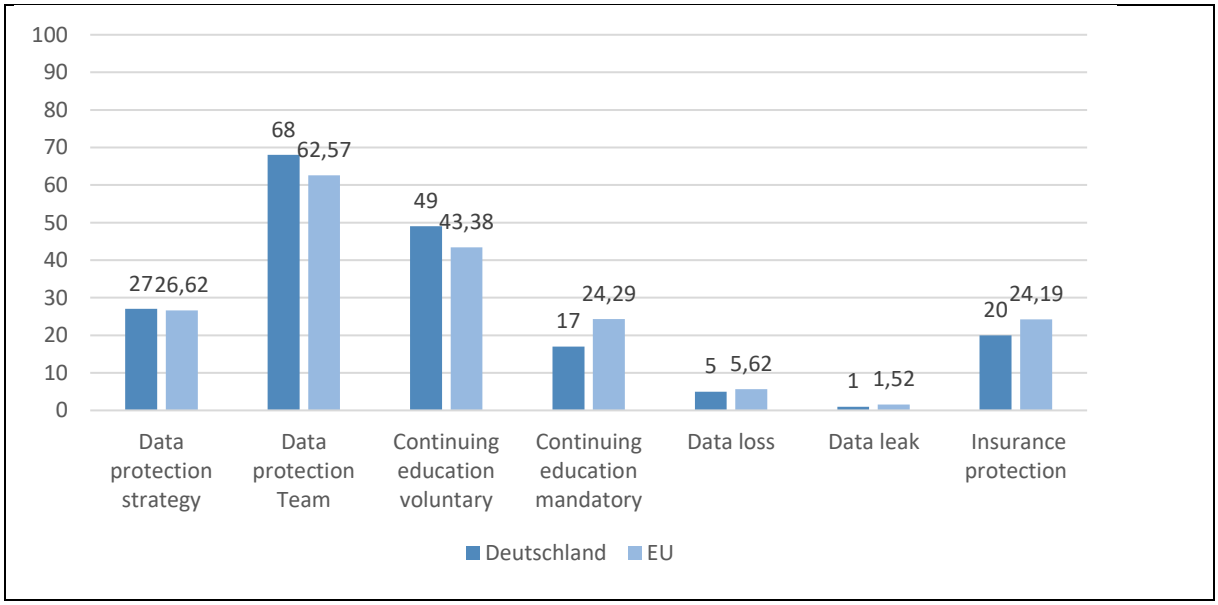

Figure 8: Composition of the data protection score for Germany and the EU average in % value

Source: heyData (2021). Own illustration.

Considering breaches of data privacy, strict punishment are being issued in Germany. With around 69 Mio EUR in fines in 2020, data breaches are being punished severely. This finding goes hand in hand with the fact that in Germany the highest total amount of data protection breaches have been reported. Especially in times of home-office throughout the pandemic, breaches have experienced a surge of around 76 % in comparison the the year before. The ramification of this finding is explained as follows: "Compared to the rest of Europe, companies in Germany for the most part behave in a very exemplary manner. However, this is also necessary. Law enforcement in Germany is handled strictly" (Milos Djurdjevic, CEO heyData, (May 2021)).

Considering this data, it is no wonder several associations have been founded which are concerned specifically with the proper implementation of data protection in the public and corporate sphere. The “Right to Informational Self-Determination” (BVerfG 15.12.1983) and the protection of personal rights against the increasing emphasis on security interests is elemental part of the work of these associations. The threat towards data protection and information security is therefore not only perceived to persist among criminal and hostile entities, but also from the federal government and its security interest.

2.4 Italy

Name of Institution	Short Description	Main Purpose	Website
Apindustria Vicenza - SMEs Association in Vicenza.	Around 1,000 members (most of them are micro/small business, with less than 20 workers). They offer services like: connection with local and regional authorities (Regional department, Chambers, regional policies); fiscal and legal services for members; training courses; specific services (i.e. for export, network, suistanibility, legal issues, EU projects, certifications, etc.). Contact person: Mr Manuel Maraschin (Director; mail: m.maraschin@apindustria.vi.it)	Some businesses (associated to Apindustria Vicenza) already have, internally, an IT and DP manager. In that case, we could verify and pilot a (part) certification process with these managers, checking the training paths through the IO3 contents (on line questionnaire). Vice versa, with external experts (consultants, IT providers, lawyers, etc.) that are supporting SMEs, we could check if the certification fits their day to day work. Apindustria Vicenza is available to organize some meetings, with local SMEs and, in the same time, propose to IT and DP managers some interviews, that could be useful for project IOs. Apindustria is not a public body; but a sort of "intermediate" organisation, that represents also local / regional collective interests. Apindustria Vicenza, as trade association, takes part into some regional working and technical tables. These meetings are also focused on professional profile, definition of specific competences, (part) certification processes, etc. So, Apindustria could support this new profile implementation, also because it represents several local SMEs. Thanks to some ESF – European Social Fund courses, Apindustria could implement, at the end of the project, also specific training paths, that could be (part) certificate by our regional training office. Timetable: the new EU 2021 – 2027 planning is, still, under discussion. At the moment, there are several technical meetings at regional level (main goal for training strategy, new contents, job profiles armonization at national and european level, ESCO priorities, etc.). But Apindustria could also aware regional authority about project contents. So, thanks to that, some project results could be implement in new programs.	WWW.apindustria.vi.it
CPV – CentroProduttivitàVeneto	It is one of the biggest training provider in Veneto Region, with almost 70 years of experience. CPV offers a wide range of training courses, for SMEs, workers, managers, consutalnts and unemployed persons. In the last 2/3 years they also organized several training course in the project topics. Contact person: Mr Enrico Bressan, (director of training department and EU projects; mail: bressan@cpv.org). He is also an external expert for the long life learning agency in Rome.	Mr Bressan has a wide experience (thanks to some regional, national and trans-national projects) in ESCO platform, Ecvet framework, EQF schemes, etc. He could support the project, exchanging his experience. Moreover, CPV is able to involve several local small businesses. As training provider, CPV built up a strong regional network, in the field of VETs and adult education. And it has a wide number of experts (for example consultants and trainers) that could check and validate some list of competences. CPV is able to involve local small business, organizing for example interviews with potential candidates and meetings (workshop) with businesses. CPV is also running a "study group" (since year 1985) focused on IT, informatics, data protection, digitalization, etc. Project interim and final results could be presented to them. As "public/private" institution, CPV sits in several technical tables at regional level (for example expert group committee for competences and job profiles recognition and assessment). It could review our regional adaptation plan and, after that, do some lobbying activities with our regional authorities.	www.cpv.org
Cesar srl	It is the training center, in Vicenza, for the local Craft association (that has more than 20,000 micro and small business). It offers a large range of training services, including courses in IT security, data protection, GDPR, etc.	Cesar works only with micro and small businesses (under 10 employees). Normally, these businesses do not have an internal expert like IT security and data protection manager or responsable. Thanks to the training courses (finanzed or not) Cesar is able to support the (part) certification process. Cesar could be involve in several phases, like: small businesses involvement; needs analysis; definition of key competences; piloting and training. In the future, they could also offer to the local companies TEBEISI certified courses, with all the project	www.confartigianatovicenza.it

	Contact person: Mrs Daniela Bucci, (vice-director of training department; mail: d.bucci@confartigianatovicenza.it).	outcomes. Cesar is part of the regional network of training centers, for micro and small businesses, composed by 7 provinces (75,000 members in total). Cesar is, very often, involved in several regional technical tables and working groups of job profiles and certification process. It could aware our regional authority on project goals and outcomes, above all for micro businesses.	
Vicenza Chamber of Commerce	It is a public body in Italy, and it offers compulsory service for all the companies. For example, each local company must be registered in the local data base (for all the business phases, from starting till closing path). Vicenza Chamber represents over 90,000 businesses, most of them are micro or small. Contact person: Mr Diego Rebesco (head of statistics deparment and promotion; mail: diego.rebesco@vi.camcom.it).	The Chamber offers a wide range of services, that includes more or less all the company needs (administrative duties, training, export, certifications, patents, etc.). The Chamber is also active in the field of job profiles recognizion, for example through the Education and Labour Ministry in Rome. It also runs interships for young persons (from the high schools) that are attending short experiences in a company, through some certified paths that, at the end, are assessed. It could be involved not only in the project promotion and dissemination (like newsletter or local workshop) but also in the certification process, thanks to the link with our national Ministry. At least, it could be informed about the project progress. But it could also set up a local (Vicenza province) working group. This body could, at the end of the project, presents the TEBEISI final (part) certification process to our regional authority, for a full recognizion. It could be our public body that verify and certify the whole regional adaptation plan, as part of its functionality and goal. In more details, it could check time table, single participant roles and, above all, validate the main plan contents, also in term of future specific legislation in the project topic, or specific needs that could be inserted in regional training programs.	www.vi.camcom.it
Proservizi srl	It is the regional training center for ConfProfessioni Veneto (that has more than 45,000 members, like lawyers, fiscal experts, notaries, consultants, etc). It offers a large range of training services, including courses in IT security, data protection, GDPR, etc. Contact person: Mrs Greta Cosentino, (director of training department; mail: greta.cosentino@proservizi.it).	Proservii has, as clients, only consultans (not company). So, they are able to involve a large number for example of lawyers that are specialized in IT security and data protection legislation. Moreover, they offer very often training courses (basic plus advanced) on GPPR and privacy code. So, they are able to check and compare project paths (for example in term of specific competences list) and what the market (companies) needs. Proservizi has already been involved in project activities. For example some members (i.e lawyers) made project interviews. They also offer financed training courses (thanks to ESF – European Social Fund, and/or specific grants from their training system, called “Fondo ConfProfessioni”). So, they are able to finance the TEBEISI profile course in the next future. Proservizi could support above all the piloting phases, involving i.e. some local lawyers with some small businesses (their clients) just for checking the project contents. But also for getting new competences in the field of IT security and data protection manager. They could also organize a specific training path for members, that includes all the TEBEISI outcomes and results. Proservi is involved, very often, in several regional working groups, in the field of training needs and competences recognizion. So, it could suggest to our regional training authority for example new inputs for the next ESF program (that will covers the 2021 – 2027 period).	www.proservizi.it
SATEF srl	It is the regional training center. It offers a large range of training services, including courses in IT security, data protection, GDPR, etc. It is also specialized in health and security sector, including elderly care centers. Contact person: Mr Paolo Pedron, (founder and director of training	Mr Pedron, the director, is an ESCCO / Ecvet expert, at regional and national level. He set up a specific training platform for competences recognizion and (part) certification. At the moment, he is running it in two sectors: health&safety and tourism. So, we could test and pilot our project contents into his platform. This test could also involved small businesses and some consultants/experts. Satef could test the project contents, for example in the field of tourism. In fact, thanks to previous experiences, the platform already exists, also in term of training path. So, TEBEISI training contents could be tested, but also a (part) certification process could be done, at regional level too. Mr Pedron takes part into some regional working groups, on “job profiles certification and	www.satef.com

	department; mail: pedron@satef.com).	assessment". So, he is able to support, strongly, our implementation phase. Due to Pedron role, at regional level, he is able to promote to our public authority the project contents and results (including the testing phases). He could also, informally, valide our "regional adaptation plan", just before sending it (for a final discussion) to our regional training and labour department in Venice.	
ENGIM Veneto	It is the biggest training provider in Veneto Region, with almost 90 years of experience. ENGIM offers a wide range of training courses, for SMEs, workers, managers, consutalnts and unemployed persons. In the last 2/3 years they also organized several training course in the project topics. Contact person: Mr Manuel Fochesato, (director of training department and EU projects; mail: manuel.fochesato@engimvi.it).	Mr Fochesato has a wide experience (thanks to some regional, national and trans-national projects) in ESCO platform, Ecvet framework, EQF schemes, etc. He could support the project, exchanging his experience. Moreover, ENGIM is able to involve several local small businesses, but also consultants, trainers and experts. Engim acts also as VETs; so part of the training courses are focused on youth, adults that need extra training and, above all, unemployed people. Engim already runs (and planned) several training platforms, that include not only training materials (i.e. on line courses for a wide range of educational needs) but also IT systems that recognazed, some time partially, specific competences. Engim can, strongly, support the job profiles implementation, in several ways: find end users (small businesses and/or consulants/experts); involve trainees (young and/or adults) that are looking for a new job specialization and, last but not least, discuss and exchange with local (regional) training authorities. Due to Fochesato role and experience, at regional level, he is able to promote to our public authority the project contents and results (including the testing phases). Engim could also share the regional adaptation plan to several public stakeholders. But also it could set up new contents in their on line training platforms, including TEBEISI contents.	www.engimvi.it
Veneto lavoro	It is the public regional agency that runs all the contents concern labour market (courses, certifications, local labour centers for unemployed people, etc). Contact person: Mr Mirco Casteller, (responsible for welfare department and EU projects; mail: mirco.casteller@venetolavoro.it).	Veneto Region, through Veneto Lavoro, runs the "Labour and Training Department"; so, the public authority that manages all the funds (i.e. ESF – European Social Funds) for workers, companies, managers and consultants/trainer. Veneto Lavoro also runs the "RRSP – Repertorio Regionale Standard Professionali" (the regional database / repertory for professional standards and qualifications). As public body, Veneto Lavoro is the most important stakeholder at regional level, above all because it runs the RRSP. And Mr Casteller is our main contact for this strategic exchange and discussion. Veneto Lavoro plays a crucial role in the TEBEISI profile/s implementation, above all in the last project phases (where the Italian partner shoud disseminate some guide lines and recommendations). As independent and public office, Veneto Lavoro can not be directly involved in the process; but it could act as "public advisor". Veneto Lavoro can validate our "regional adaptation plan" step by step. In the meaning that we could inform, since the beginning, Veneto Lavoro about project progresses and, at the end, propose this new job profile that could be (part) certificate and insert in the regional database for professional standards (RRSP).	www.venetolavoro.it
INAPP - Labour Ministry	It is the new agency at national level, that runs and check all the national (and European) projects that are connected with competence assessment and certification. Contacts: urp@inapp.org (or some specific departments, like atlante_lq@inapp.org)	Like the previous mentioned stakeholder (Veneto Lavoro) INAPP could strongly support our project, in term of exchange and suggestions for the whole cerfication process. In particular, INAPP runs the new "Atlante del lavoro e delle qualificazioni" (Atlas of jobs and qualifications). The Atlas is the overall (national) database / repertory for the professional standards and qualifications. It also includes profile for students (high schools and Universities) and guide lines for VETs and training centers. Recently, INAPP launched also the "Atlas for professionals" (like consultants, trainers, lawyers, etc.) and they could check the project progress in term of "TEBEISI IT secury and DP managers" new profiles. And, in the middle term, insert and promote also this new new profile. INAPP could also check the project contents in term of future ESF – uropean Social Funds - new training courses	www.inapp.org

		(program: 2021 _ 2027) based on TEBEISI outcomes. INAPP could be informed about the progress, at regional level. And check, giving some feedbacks/suggestions, in term of coherence and project sustainability in the middle term. And also it could assess the training materials, including above all the (part) competence certification process, at least at national level. NAPP runs dozens of working groups at national level. Many times, these groups are also running at regional level. So, we could meet and discuss with some group members, proposing them or regional adaptation plan, before project closing.	
AIPSI	Associazione italiana dei professionisti sicurezza informatica (the Italian association for IT security professionals and experts). It is the Italian chapter of ISSA, an international non-profit organization of professionals and experienced practitioners. With the active participation of individual members and their chapters around the world, AIPSI, as a chapter of ISSA, is part of the largest non-profit association of security professionals with over 13,000 worldwide. Contact person: Mrs Yvette Agostini (Director, info@aipsi.org)	AIPSI is one of the most important italian association for IT security expert. But it works also with data protection managers. If offers a large range of services, useful for TEBEISI project, like: surveys and researches, reports, training and consultancy and, of course, (part) assess and certification activities for the professional profiles. Most of their courses (free of charge of for payment) already got the certification from a national or regional body. It also part of a wider international network; so it could give us a larger vision and further information. AIPSI could check the project contents and assessment phases. In particular, they could accept and verify some new training materials, for example some specific competences (like soft skills or personal skills). AIPSI has several members that come from Veneto region too (there is also a local office in Venice; most of the local members are informatics engeneers). With them, we could exchange some contents and, above all, check the final versions. Moreover, our project could link Clusit members (that are professionals) with SMEs. AIPSI already takes part into several technical working groups, at national level (Ministry of Innovation and Education in particular) and in several regional task force. In particular, their reports and pubblications are the scientific basis for further legistative improvement in the field of (new) job profiles recognizion. For our Region, the local AIPSI president or director could represent the scientic and technical experts.	www.aipsi.org
CLUSIT	Associazione Italiana per la sicurezza informatica (the Italian association for IT security). CLUSIT Italy was created on the basis of the experiences of other European computer security associations such as CLUSIB (Belgium), CLUSIF (France), CLUSIS (Switzerland) CLUSIL (Luxemburg) which have been a reference point for computer security in their respective countries for over 20 years. Main goal: Spreading the culture of information security to Companies, Public Administration and citizens. Contact person: Mr Gabriele Faggioli (the President; president@clusit.it)	Clusit is one of the most important italian association for IT security expert. But it works also with data protection managers. If offers a large range of services, useful for TEBEISI project, like: surveys and researches, reports, training and consultancy and, of course, (part) assess and certification activities for the professional profiles. Most of their courses (free of charge of for payment) already got the certification from a national or regional body. Clusit could check the project contents and assessment phases. In particular, they could accept and verify some new training materials, for example some specific competences (like soft skills or personal skills). Clusit has several members that come from Veneto region too (most of them are informatics engeneers). With them, we could exchange some contents and, above all, check the final versions. Moreover, our project could link Clusit members (that are professionals) with SMEs. Clusit already takes part into several technical working groups, at national level (Ministry of Innovation and Education in particular) and in several regional task force. In particular, their reports and pubblications are the scientific basis for further legistative improvement in the field of (new) job profiles recognizion.	www.clusit.it
Padua University – informatics and computer	In the last years they made several surveys on project topics.Contact person: Prof. Antonio Scipioni (scipioni@unipd.it).	Padua University already organizes second level masters on project topics (data protection manager, IT security expert, etc.) and also training courses. Their training contents and paths could be useful for the competenteces and job profiles selection. They could involve managers, experts and SMEs,	www.unipd.it

engineering" department.		for example for making inteviews, workshops, etc. As University, they could "guarantee" a scientific approach and the right methodologies. As athenaeum they could involve also several departments (economy, law, IT - informatics, management, etc.). The university is a public body, that takes part into several regional steering committee and working groups, including also expert groups on project topics. So, if they are aware on project progress they could support the certification process at regional level.	
APCO – Italian association of managemen t consultant	It the Italian association for management consultants, founded in 1968; now it has over 400 members. APCO offers several services for members, like: training, networking initiatives, lobby with institutions, etc. Contact person: Mrs Cesara Pasini (President; mail: presidenza@apcoitalia.it)	APCO has several "communities of practice" that are focused in different topics. In particular, two of them (digital transformation / innovation manager and compliance / ISO standards) could help us in the part-certification. APCO promoted a special national law (nr. 4, year 2013) that recognized also consultants that are not registered in professional body (by the law); but that they have a certification profess and a continuous training. APCO is available to organize some meetings (also on line), with some members that are working on project topics. APCO is not a public body; but a sort of "intermediate" organisation, that represents also local / regional collective interests. For example, there is the "North East" delegation (Veneto, Trentino Alto Adige and Friuli Venezia Giulia area) that could be involve in some project activities. The local delegation (Veneto region, Mr Paolo Ferrarese as coordinator) could do some lobby with our local authorities (Region, labour and training department).	www.apcoitalia.it

Table 4: Stakeholder from Italy

The GDPR in Italy has been officially applicable for some time now, exactly since 25 May 2018. Then, on 19 September 2018, the text adapting the Italian legislation to the General Data Protection Regulation, namely Decree 101/2018, came into force.

Italian GDPR: where do we stand, after three years?

In June 2021, the "Privacy supervisory authority office" has published a report on its activities in the three years of enforcement of the Regulation and it has emerged that there has been an increase in the awareness of data subjects in relation to their rights with approximately 27,192 complaints and infringement reports to the Garante. (GDPD 2020) The high number of reports, about 24 per day, 365 days a year for three years, shows that the adoption of the GDPR has certainly increased the awareness of data subjects in relation to the existence of their rights and the request for their protection.

The number of notifications increased to 2839 in the quarter between 1 January and 31 March 2021, a sign that the pandemic year with the digitization of many activities has also led to greater user attention to the issue of personal data protection.

Similarly, there were 3,873 notifications of data breaches (about 3.5 per day), which are few when compared to statistics on cyber-attacks, but nevertheless indicative of the importance of adopting security policies and tools to help prevent them. A fundamental aspect, in any case, is staff training and awareness-raising on the subject of security and on the behavior to adopt in the event of requests that do not comply with company procedures.

The names of 59,838 Data Protection Officers (also known as DPOs) were communicated, and not all of them by Public Administrations which, under the Regulation, are obliged to appoint a DPO. This shows how the need to have a figure

of coordination, surveillance and contact between the supervisory authority, the data subjects and the data controller is seen as an important requirement.

On the sanctions front, 654 proceedings were carried out in Europe for a total of €283,757,083, (source), looking at the statistics divided by countries, Italy ranks first for the total amount of sanctions imposed for €76,298,601 in 79 measures, confirming the activity of the Italian Garante and the attention with which complaints and reports are handled. This count, of course, only considers sanctions imposed under Article 83 GDPR and does not take into account any damages or compensation paid to data subjects whose rights have been violated. As stated by the members of the Supervisory Authority on the anniversary of the EU Regulation, there is still a long way to go to combine the digitisation of Member States with secure infrastructure management. The increase in the perimeter of vulnerability of companies, due to the more or less forced adoption of remote working solutions, requires owners to rethink data flows and security procedures within their organisations.

But what does this mean for businesses in our country? Fortunately, the trend seems positive. Almost two years after its full application, significant progress is being made in Italy in terms of compliance with the regulation, with increases in the budget available to organisations and growth in maturity, in terms of the concreteness of projects and targeted organisational changes.

However, the complexity and importance of the subject matter require continuous efforts by companies to adapt to the principles imposed by data protection legislation and to respond to requests from the authorities. In this regard, the first fines for breaches of the Regulation have been imposed in several European countries. In Italy, on the contrary, the attitude of the Supervisory Authority was initially accommodating, also due to delays in the election of the new College of the Supervisory Authority. However, the most recent period has seen an intensification of checks and inspections and the application of the first sanctions provided for by local and supranational data protection legislation.Thanks to the research conducted by the Cyber Security & Data Protection Observatory, we can see how this legislation is changing the Italian context.

The state of compliance with the Italian GDPR

In order to explore the changes taking place in Italian companies with regard to Data Protection, the Observatory considered four aspects:

- status of compliance projects
- dedicated budget
- actions implemented
- Critical issues encountered

The study shows that almost all Italian companies have implemented or perfected GDPR compliance projects. More than half of the organisations said they complied with the requirements of the legislation and, at the same time, the number of

companies that said they were not aware of the implications of the GDPR has decreased.

On the latter point, however, it should be pointed out that these are companies where the issue of data protection has not yet reached the top, but is nevertheless known to specialist functions such as IT Security, Legal and Compliance. Another positive sign of the maturity and awareness of the GDPR in Italy is the low percentage of companies (5%) that are still in the phase of analysing the requirements and defining compliance plans, whereas two years ago this share reached 34%. The picture is also positive in terms of the budget dedicated to GDPR compliance measures: 45% of Italian companies have increased their dedicated budget. While this number is positive, it is also true that the focus has yet to shift to specific activities such as periodic audits, updating procedures and security and data protection technologies. (Andrea Antonelli 2020)

DPR compliance actions

In concrete terms, what are Italian companies doing to comply with the GDPR? It should be remembered that the process of compliance must necessarily be composed of several stages, which currently have different levels of adoption:

- Creation of the processing register (85%): mandatory creation of a register where to keep track of all processing operations carried out;
- Identification of roles and responsibilities (81%): identification and contractualisation of all those responsible for processing;
- Modification of forms (76%): updating of forms according to the requirements of the GDPR;
- Data Breach Notification procedure (68%): process for notifying the Supervisory Authority of breaches of confidential data;
- Definition of security policies and risk assessment (66%): adoption of measures to ensure that processing complies with the Regulation;
- Data Protection Impact Assessment (56%): mandatory Data Protection Impact Assessment (DPIA) when processing is likely to pose a high risk to the rights and freedoms of data subjects;
- Implementation of processes for the exercise of data subjects' rights (54%): actions to enforce the rights granted to data subjects by the processing. (Andrea Antonelli 2020)

In addition to these actions, it is also necessary to consider the inclusion of the figure of the Data Protection Officer (DPO) in companies. This figure, whose appointment is provided for by the GDPR in a number of cases, is present in 65% of **organizations**. This figure is certainly positive, as it reveals an increase in the number of companies that have introduced this figure.

What critical issues does the GDPR entail for Italian companies?

If it is true that the picture on the state of compliance with the Italian GDPR is generally positive, it is also true that organizations have encountered some difficulties. In fact, many companies are still experiencing difficulties from an organizational point of view, for example in identifying roles and responsibilities within the company, while others report a significant slowdown in day-to-day activities.

However, these negative elements are of little account compared to a mature scenario where Italian companies are showing themselves to be not only oriented to face the challenges in terms of data protection, but also aware of the whole issue.

2.5 Lithuania

Name of Institution	Short Description	Main Purpose	Website
Alytus Business Consulting Centre (AVKC)	Alytus Business Consulting Center (AVKC) is the first business consulting center in Lithuania, registered on 13 May 1993. as a non-profit organization that was subsequently re-registered as a public body. Alytus Business Consulting Centre – Alytus Regional Development Strategy participant in international development cooperation in regional development with the Swedish Jonkompingo County, Poland, Denmark, Hungary, Italy regional authorities, Ministry of existing business development agencies, Alytus county municipalities and associated structures of the initiator.	Alytus Business Consulting Center's mission – to promote and develop small and medium-sized businesses, providing business training, counselling, information, new business development initiatives in the development and implementation of networking development in Alytus region.	https://www.avkc.lt/lt/
Association of Heads of Municipalities Social Welfare Institutions	Association of Heads of Municipalities Social Welfare Institutions - an independent, voluntary non-profit organization, comprising 30 municipalities care institutions	Purpose of the Association - to help solve problems of social care users of all groups of people by improving their quality and integration into society.	http://ssgivasociacija.blogspot.com/
Law firm ALIANT Tarvainyte Vilys Bitinas	The ALIANT® team in Lithuania provides integrated legal services in all business management and development processes and business disputes in national and international court institutions. They also work in the field of data protection	The ALIANT® team in Lithuania provides integrated legal services in all business management and development processes and business disputes in national and international court institutions.	www.aliantlaw.lt
LDAPA - Lithuanian Association of Data Protection Officers solutions.	The priority of LDAPA members is to create an innovative, next-generation, non-commercial platform for personal data protection professionals to share specialized legal knowledge, good practices, practical and new	The priority of LDAPA members is to create an innovative, next-generation, non-commercial platform for personal data	https://ldapa.lt/

		protection professionals to share specialized legal knowledge, good practices, practical and new	
Information Security Center	In order to achieve the operational objectives of the Center, data controllers and processors shall be consulted on the implementation of appropriate technical and organizational measures for data protection. Data subjects are consulted on the implementation of human rights in the field of data protection.	The goal of the Information Security Center is to improve public awareness of the issues of secure personal data processing, information protection and cyber security.	https://infosec.mobi/

Table 5: Stakeholders from Lithuania

The Law on the Development of Small and Medium-Sized Business of the Republic of Lithuania (2017) specifies that small and medium-sized business entities are medium-sized, small and very small enterprises that meet certain requirements (number of employees, income, independence) and natural persons entitled to self-employment. commercial and other similar activities. During 2019, the number of small and medium-sized enterprises increased by 0.4 percent. (registered 11153). The largest share - 83% - of SMEs were very small enterprises (0-9 employees). Small enterprises accounted for 14% (10–49 employees), medium-sized enterprises (50–249 employees) - 3% in 2019. Over the year, the number of people working in SMEs increased by 2.2%.

Despite progress in the small and medium-sized business sector, improving the general business environment and reducing barriers to market entry, the dynamics of entrepreneurship in the Lithuania remain weak. Administrative procedures for setting up new businesses are complex, and entrepreneurs lack start-up capital and management and financial skills, marketing and export skills and information. Decisions to overcome a pandemic crisis, boost the economy and improve the business environment are difficult to implement and do not produce the expected results.

TebeISi project research in Lithuania shows that too little attention is paid to this issue. Insufficient attention is paid to the public sector and small and medium-sized enterprises. The lack of attention is related to a lack of funding. Greater attention to information security is being paid by the portion of the society that is exposed to information security in one way or another. According to experts, a lot of attention is given to state institutions. As it comes to business – the focus is way less significant, since not many people understand the issue fully. Public attention to information security is also increasing by following public security incidents. The research shows that SMEs do not pay enough attention to in-house training. This usually depends on the initiative of the employees themselves in finding and participating in the training. Recently, experts have also linked the lack of training to the difficult situation of the

COVID-19 pandemic when many companies have been suspended and were focused on survival.

A quantitative study conducted by M. Lipinskienes (2019) A quantitative study conducted by M. Lipinskienes (Austrian Press Agency 2020) (2019) on the implementation of the General Data Protection Regulation in Lithuanian companies revealed that the companies participating in the survey in Lithuania, which process personal data themselves and entrusted data processing to a data processor, are sufficiently compliant with GDPR. During the questionnaire survey, the respondents answered the statement: “the company I represent effectively implemented the requirements of the GDPR ” from 1 “strongly disagree” to 100 “strongly agree”. The answers were coded in the SPSS program on an interval scale and the average score of the respondents was calculated. A total of 77 respondents answered the statement, the lowest rating was 0, the highest was 100, and the average score was 77 on a 100-point scale, which means "I agree". The respondents most often rated their companies with 100 points - 23 respondents, 8 respondents - with 95 points, 6 - 90 points, 7 - 85 points, 6 - 80 points. Up to a score of 80, answers are rated "strongly agree", which means full compliance with GDPR. There were 50 such companies out of 77 respondents, which is 65%. More than half of the companies' representatives agree with the statement that the company complies with the GDPR standard as "completely agree".

The survey revealed that, in the respondents' opinion, the regulation is rather abstract, laconic, difficult to read and difficult for non-legal professionals to understand. Companies that process the data themselves lack the knowledge and understanding of GDPR, which leads to ignorance and hesitation. However, in-house training is important and significant for every employee of the company and for the company itself. In order to comply with the GDPR, the data controller must find out what personal data is being stored, where, for what purpose, for how long, how it is being processed and stored. Only by understanding what you have will the data controller know how to behave and manage. This has been confirmed by the TebeISi project desk reseach (IQ1), data processing and personal data protection assessments as an opportunity to identify redundant information and review business processes. In this way, efficient business processes would be recognized in companies, inefficient and redundant process stages would be reduced or eliminated. This would help companies to ensure the security of information and the protection of personal data.

Training Situation

In Lithuania, there is a wide range of training (1.5 hours to several days) on data and information security. Most often training is provided by private institutions, for example: Cyber Security Academy founded by UAB “Hermitage Solutions” that aim is to train IT specialist who is able to solve complicated cyber security issues in a timely and efficient manner and to assess the vulnerability of his organisation's IT infrastructure. UAB “Atea“ that is the leading Baltic supplier of IT solutions and services and assist

customers with specialist competences, products, services and solutions within IT infrastructure, software development and security. NRD Cyber Security that is a cybersecurity technology consulting, incident response and applied research company. The company focuses on services for specialized public service providers (law enforcement, national CERTs, telecoms, national communication regulators, national critical infrastructure), the finance industry and corporations with high data sensitivity. UAB "Competence Development", that offer training courses to prepare for the most popular certifications, which are the basis for work with other manufacturers' equipment, so these certifications are often preferred by employers not only in Lithuania but also abroad.

Training on information security is organized for different target groups: both beginners, advanced IT users and IT professionals. The main topics of information training are: “Information Security Training”; “Cyber security training”; “Information security training for non-professionals”. A separate group of information security training focuses on IT professionals. They are trained on topics such as: "Basics of cyber security"; “Hack IT to Defend IT”; Ethical hacker practitioner; "Safe programming"; "IT security practitioner"; “Cyber security incident management” and “IT security awareness training”.

Professional training at different levels on data protection topics is mostly for IT professionals. The main topics of such training are related to the Protection of personal data in the context of GDPR requirements training. Training on data security is also organized for corporate lawyers, administrators, managers, staff managers. Such training is introduced to the GDPR; “Protection of personal data and responsibility of GDPR violations”; "Protection of personal data and violations of personal data legislation in 2018".

2.6 The GDPR and economic activities

With the initiation of the GDPR in 2018, the European Commission set out coherent guardrails ensuring the fundamental right to data protection and providing grounds for the realization of the Charter of Fundamental Rights of the European Union. The GDPR spurred many other countries around the globe to become active in their data protection regulation and follow the path of the EU and influence the stance and behaviour of all stakeholders to the benefit of the European citizens.

Nonetheless, the adoption of the European Data Strategy (European Commission 2020a) encounters several obstacles, reported by the European Commission in a communication regarding the implementation of the GDPR (European Commission 2020b). Meanwhile the general awareness for the value of personal data has increased among citizens and procedural rights have strengthened the ability to report cases of misconduct, especially in the cross border usage of data shortfalls remain. In this regard, the right of data portability between services for the benefit of public goods usage is to be explored and limiting factors uncovered. (European Commission 02.06.2020).

Concerning the need of SMEs, the GDPR has increased the possibilities of free flow of data within and improved flow of data with firms without the EU and thereby fostering innovation and economic activities. SMEs, however, need to tackle the relatively demanding implementation of the GDPR in order to participate from these new opportunities – as the risk of data breaches does not decrease with the size of an operation. Efforts to provide practical and easy-to-use tool for SMEs are therefore to be increased. The Commission aims to support specifically SMEs by providing templates for contracts and clauses which comply to the GDPR.

Ultimately, the successful implementation is reflected in the successful enforcement by the national data protection authorities. As can be seen in Figure 9, large differences become apparent across the member states.

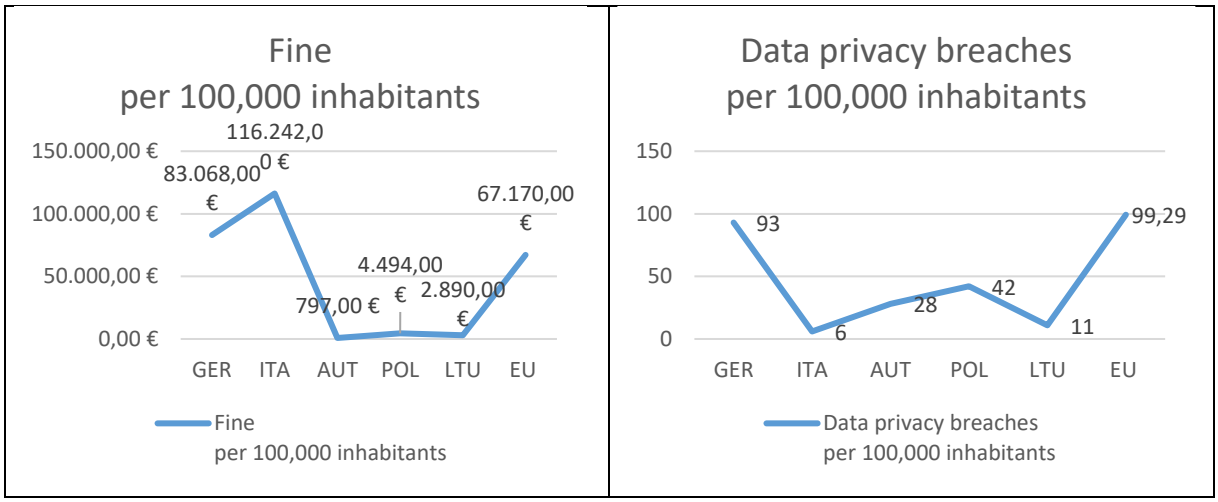

Figure 9: Enforcement of data protection law in the member states. Net values per 100.000 inhabitants.

Data: heyData (2021). Own illustration.

Meanwhile all countries remain below the EU average of total data breaches per 100.000 inhabitants, which is dominated by the large numbers reported for Ireland (245), Denmark (325) and the Netherlands (382), significant spikes can be reported for the fines paid. To better understand the relationship between amount of fines paid and numbers of violations, the net values have been adjusted for purchasing power parity[2] to ensure comparability between the countries. The results illustrate that Germany is close to the average detection rate of the EU, meanwhile Italy, Austria, Poland and Lithuania lie well below. Similar findings can be observed for the paid fines, with the prominent exception if Italy, where fines are being paid almost doubling the European average and surpassing those in Germany by around 40%. This spike lead to further analysis, by calculating the costs of a data breach adjusted by the Purchasing Power parity Figure 10 (left) and the again for the risk of detection, whereas the average risk level was calculated by setting the EU average value to 1.

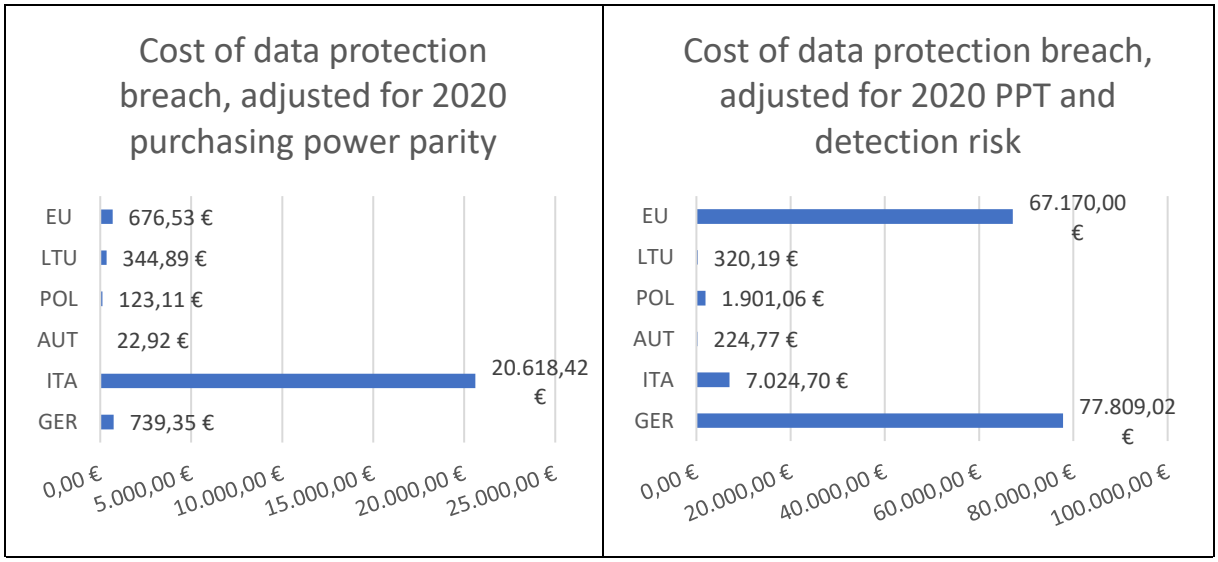

Figure 10: Cost of data protection breaches adjusted for purchasing power parity and detection risk

Data: heyData (2021). Own illustration.

Meanwhile the observation of the ppt adjustments makes clear that per case reported, an extreme spike is observed in Italy, the risk adjustment makes clear that these are very few cases with big fines. Nonetheless, it can be seen that large discrepancies exist for the risk-cost calculation of data protection breaches, with only marginal punishments in Austria, Lithuania and Poland and severe punishments in Germany. It can therefore be concluded that law enforcement still has a long way ahead of being equally effective in all member states.

Considering the individual situations in the partner countries, specifically for SMEs challenges in the implementation process become eminent. Especially a lack of time and a lack of resources has been identified as primary reasons for the sluggish implementation. Especially the alignment of processes and control for GDPR significant information in the firm are areas in which across all countries SMEs have

[2] The data has been extracted from Eurostat 2021.

room for improvements. Ultimately, the question of proper implementation is closely connected to the availability of staff and the need for practice oriented training courses. The strong demand for further education courses (both voluntary and mandatory) illustrated the market gap for concise, transferable, and transparent courses, as suggested by the TeBeISi research agenda.

2.7 The weakest link – the role of employees and Privacy Calculus

In light of the efforts by firms, non-governmental organizations and public authorities to bring the GDPR into action, a successful implementation faces the same restraints as the implementation of information security: the human factor. As has been shown in chapter 2.6, a strong demand for personnel and especially further training courses exists. Employees, being the main cause of information loss and data protection breaches, play a pivotal role in the conduct and compliance of data protection and information security.

Firms have many possibilities to ensure the protection of their data, be it on an organizational or a technical level. From an organizational standpoint, they can roll-out processes which ensure that only a marginal amount of data is being collected, that physical and digital storages are secured, that the access to data is restricted to relevant personnel etc. The analysis and implementation of these measures lie within the authority of the information security officer in conjunction with and backed by the lead of the firm.

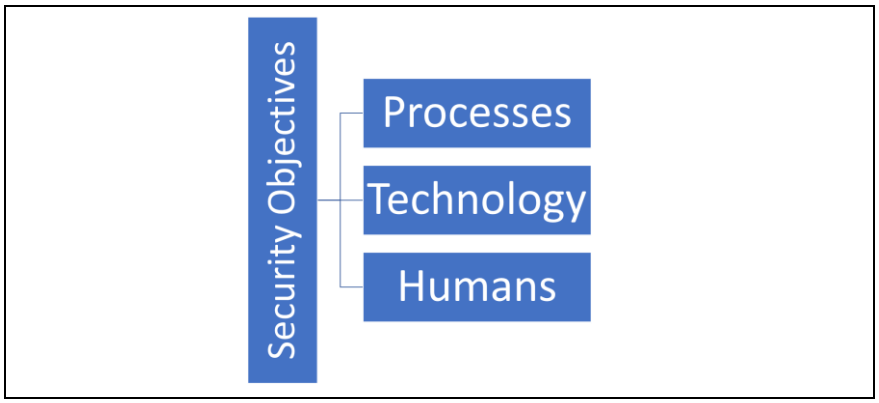

Figure 11: Dimensions of Risk to Security Objectives

On a technical level, programs and applications can be designed which ensure the compliance with data protection law and the specific regulations of the firm, i.e. privacy by design. Service providers have started to make business model out of Software as a Service (SaaS) platforms, implementing Privacy as a Service (PaaS). This way, with the consent of the user, storage and processing of information is focused on proper conduct according to the individual requirement. Further, the importance of secure software has experienced a strong increase over the past years, as leakages become easier known to the public and can hurt the reputation of the companies. Consequently, firms have gained an interest in designing secure software and building trust among their users – yielding a competitive advantage on the market.

Finally, firms need to respect the human dimension in the context of protecting their know how and critical data. It is the user and actor in the firm, operating machines and technologies, carrying out tasks and supervising processes. Meanwhile both technology and processes dispose of a very high reliability, employees tend to make mistakes, as they are subject to “bounded rationality” (Simon 1990). In fact, around 88% of data breaches or information loss can be attributed to human errors, rendering

this dimension the most important dimension in order to ensure the safety of data in a firm. (Tessian 2021)

In short, the concept of bounded rationality rejects the assumption that humans thought, behavior and action is guided by complete rationality, as this would require unbound cognitive capability to process every information available immediately and take fully informed decisions. Instead, it is assumed that humans maximize their individual utility, i.e. they chose an action which meets their own perceived need the most (so called “Satisficing”). Finally, a person might also come to the conclusion that they lack information to take decision, but that the search for this information would entail a significant amount of time and energy. Consequently, the person decides to take an action with incomplete information, as the opportunity costs (time and energy) exceeded the utility of having that specific information.

Among these actions, setting up easy passwords (or writing them into a post-it), delaying security updates, storing sensitive information in lockers, using that stick found in the elevator are only a few of the ill-advised consequences. The absence of complete information and the perceived high opportunity costs in moments of rush and pressure are increasingly exploited by social engineering attacks, in which an intruder creates a scenario via mail or via phone, which evokes urgency to take action in the hope that the employee leaves aside security protocols, providing critical information (e.g. passwords, financial information etc.) voluntarily.

Unfortunately, adhering to proper conduct in the daily working life takes up extra energy – which is often a scarce resource in productive or hectic work environments. In the background of established working routines, changing attitudes, believes and finally behavior pose a large challenge to both the firm, but also to its employees. Hitherto, teaching, training and sensitization of employees with the end to raise awareness for the constant threat to the firms most valuable assets – its know-how and its data – is more important than ever before. And with decreasing difficulties to launch any sort of attack, more and more SMEs need to face a new reality: they are already, or a most likely will be, subject to targeted attacks. So, what can be done?

3 TeBeISi Strategy

The project TeBeISi has analyzed the situation of information security, also with respect to the implementation of the GDPR, on a firm level in the partner member states. After reviewing currently existing job profiles, formal qualifications and certifications a match was conducted of currently existing, transferable competences and the requirements generated from the quantitative and qualitative analysis.

3.1 Connecting Higher Education and Work-Based Training

After reviewing all information gathered via quantitative and qualitative research, the project came to the conclusion that Information Security is predestined to provide for a mix of vocational training and higher education. There are three reasons feeding into this idea:

1. Operational Activities: Most of the tasks required to be carried out in an SME are of a rather routinised nature. The degree of knowledge transfer and recontextualization remains low, as technology and processes remain on a standardized level, with firms making use of standardized EDP software and communication channels. Most SMEs can achieve a significant increase in their security level by sticking to the 20:80 rule (or similar) – they reach 80% security by doing 20% of the work necessary to reach 100%. Of course, this is not possible considering data protection, which is mandatory by law and for which firms are obliged to meet the demands of the GDPR. The consequences of this finding are manifold: firms need to take into account whether they want to reach for a specific certification (due to the nature of their product, requirements by the market etc.), whether they possess resources which require more than routinized protective measures etc. Thus, SMEs often find themselves in a position where the structural adherence to basic security measures provides for a significant increase in overall security level and a significant decrease of risk exposure in a cost-effective trade-off.

2. Legal Obligations: Despite the possibility of conducting routinised tasks in a structured work environment, some aspects of information security also touch on legal aspects, especially concerning the implementation of correct data processing following the GDPR. Due to the complexity of dealing with national regulations, responsible personnel is required to possess the competence to deal with legislation and the correct implementation. This responsibility involves a high degree of capability to recontextualize and transfer abstract knowledge in a working environment. Meanwhile the degree of complexity remains overseeable concerning the technical end of information security described under (1), the legal end demands diligent training and execution to comply with the respective laws.

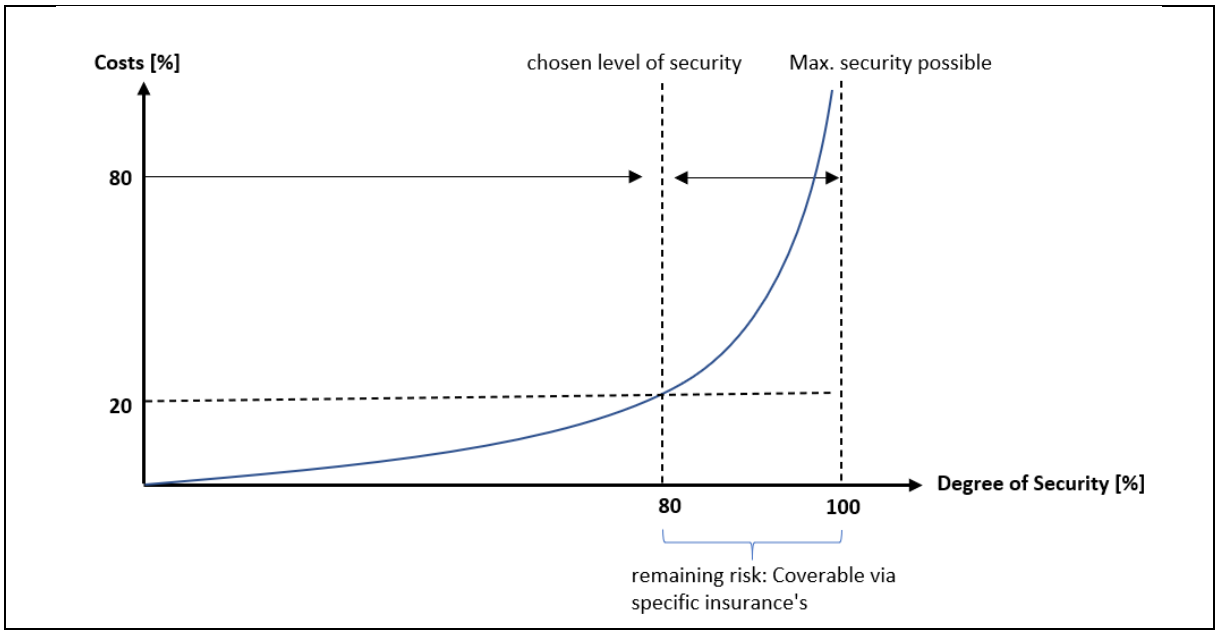

Figure 12: Cost-Security Trade-off of Information Security Investments

3. The work of Information Security responsibles requires manifold social skills. As described under 2.3, the largest threat toward the security of a firm is represented by its employees. Changing the attitude of coworkers, influencing their working routines and establishing a culture of information security in the firm pose, arguably, the largest challenge in the implementation of an information security system. The person in charge is required to activate, collaborate, guide, mentor and reconcile employees, managers and information security. It does not come as a surprise that firms appreciate professionals with experience on the job – and value practical experience higher than any formal qualification (cf. Study "Information Security Education for SMEs"). Receiving a hands-on education teaches the pitfalls in the daily cooperation with colleagues, and the skills to productively interact with the stakeholders in the firm.

Information security education, when existing, currently focuses strongly on the teaching and training of technical competences, either in the domain of IT or law. Gaining practical experience, especially effective communication strategies, only rarely finds its way into educational curricula. TeBeISi therefore suggests to connect the best of both worlds, and to provide education by means of vocational education and training and higher education.

3.2 Making use of European Instruments

The connection of vocational education and training and higher education has been defined by the European Commission to be feasible within the European Qualification Framework (EQF). Further, the European Credit System for Vocational Education and Training (ECVET) shall be deployed in order to provide for transparency and comparability in Vocational Education and Training. Finally, referring to the European Skills/Competences, Qualifications and Occupations framework (ESCO), single competences can be formulated in a way which make them reusable and recognizable in different vocational contexts.

The usage of European instruments sets apart a transparent certification process from the already existing, disorganized market of certifications from private providers. It needs to be reiterated that manifold credentials exist, also in the domain of SMEs, however it remains unclear to which extend common quality and quality assurance standards are being used, yielding a lack of transparency and transferability across countries. The backlog to European wide systems of accreditation, quality assurance and competence standards allows for a broad and transparent roll-out of certifications across educational systems and institutionalized certification landscapes.

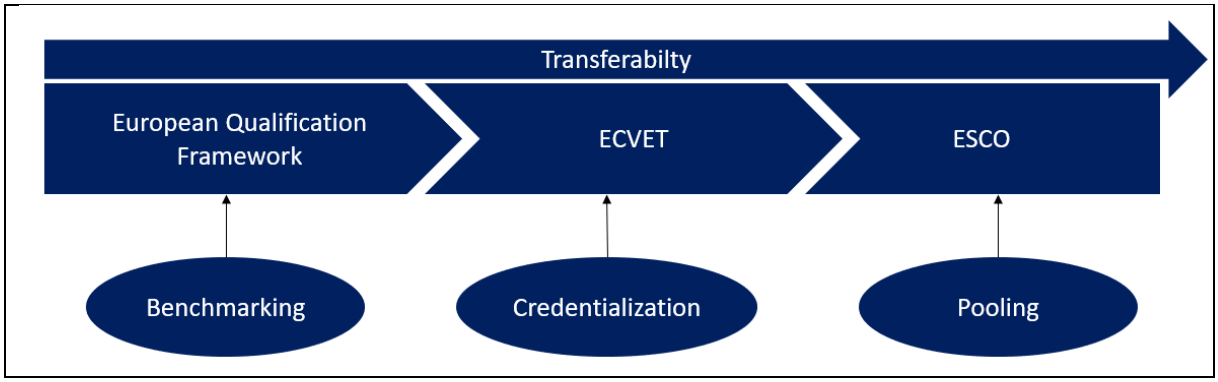

Figure 13: Transparency Intruments for VET in the EU

In brief, these instruments support the EU-wide dissemination of competences and qualifications. The EQF as a benchmarking system categorizes qualifications according to their underlying skills, competences and autonomy and provide the possibility to fit every qualification from the different educational systems into a single reference scheme, which makes the different qualifications comparable across different educational contexts. ECVET, meanwhile, provides the basis to bundle learning outcomes into learning credits, providing an insight into the volume and depth of learning behind a qualification. Further, it supports quality assurance, provides continuing education possibilities in regionally specific contexts and supports the recognition of vocational qualifications in different systemic or national education pathways. Finally, ESCO represents a unifying database which brings together existing qualifications and competences from across the EU. By reverting back to this database when creating new curricula, it can be ensured that competences are understood in different learning contexts.

3.2.1 European Qualification Framework

The European Qualification Framework sets out a systematization of formal qualification among the educational systems in the European Union.[3] The end of this framework is to make qualifications comparable among countries, and, consequently, increasing the understanding about the value of a qualification in the foreign. As educational systems vary widely among the Eu member states, the EQF can be used as a reference to ensure the equivalence of taught competences. In the TeBeISi context, EQF level 5 has been identified to provide valuable opportunities for firms and learners.

The learning outcomes relevant to Level 5 are		
Knowledge	Skills	Competences
comprehensive, specialised, factual and theoretical knowledge within • a field of work or study and an awareness of the boundaries of that knowledge	a comprehensive range of cognitive and practical skills required to develop creative solutions to abstract problems	exercise management and supervision in contexts of work or study activities where there is unpredictable change review and develop performance of self and others

Table 6: EQF Level 5 Learning Outcomes - Knowledge - Skills - Competences

Source: European Commission (2008)

Considering a key caveat of the project, that most personnel available is likely to be overqualified for the needs of SMEs (which is also reflected in existing occupational profiles in ESCO), suitable means have to be found to align the inherent complexity of the tasks of information security (i.e. IT know-how and legal knowledge), and minimum requirements by SMEs in order to address new learners in the field. It can be concluded that due to the nature of some tasks, especially those related to non-standardized activities or involving legal competences, some elements of information security education for SMEs need to be rooted in higher education, which enables learners to operate in a less structured and more independent environment. Specifically, competences related to law, i.e. mostly GDPR, fall into this category.

The use of EQF 5 provides several advantages which can be exploited. First, it provides a ground for many employees with EQF 4 qualification to find an entry into continuing education. Consequently, partial validation on this level can be facilitated by the recognition of prior work experience, non-formal and informal learning. The connection to EQF 6 bridges the gap and adaptability for higher education institutions, which aim to provide either a full qualification in the context of information security or additional qualification to their students.

[3] c.f. Cedefop 2009

3.2.2 ECVET

From a functional perspective, the learning outcome-oriented operationalization of competences represents a shift in perspective from “What do I want to teach?” to “What should learners learn?”. The result of the learning process represents the focus of the learning process and provides learners with a clearer view on their own learning progress. With the usage of a transparent credit system, several positive externalities can be realized which differentiate the modularized education path from existing certification systems.

The dispersion of the TeBeISi competence profile of an information security and data protection officer in SME into modularized learning fields (c.f. “Curriculum”) facilitates the modularization of learning fields and the application of credit transfer systems like ECTS or ECVET. ECVET. The modularization (micro-credentialization) provides several advantages, illustrated in Figure 14, leading to increased transparency, mobility and trustworthiness of the partial qualifications. The modules can both be used for training and education purposes of employees or students or used as a means of partial validation by making the certification process available to lateral entrants from the field of information security.

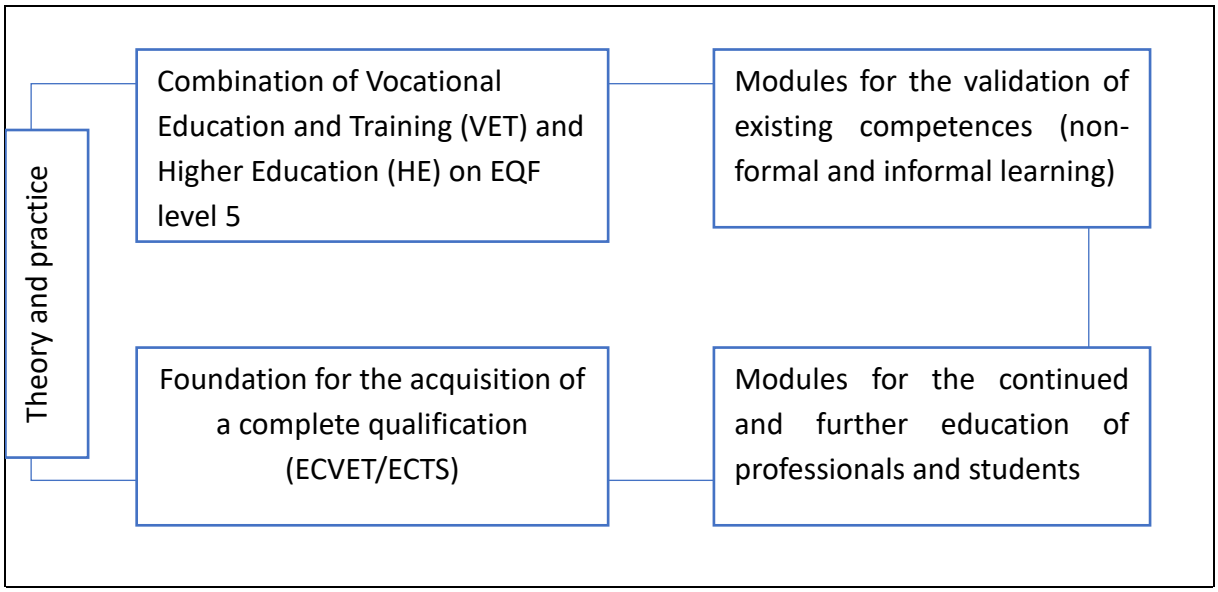

Figure 14: Advantages of modularized qualifications

Considering existing validation systems, trustworthiness plays a crucial role in the acceptance of the certification process among employers and training providers. There, in addition to the existing quality assurance standards (e.g. EQAVET), specific details concerning competence assessment need to be taken into account in order to ensure the highest possible validity of the validation procedure.

3.3 Measuring Learning Outcomes

The measurement of learning outcomes remains a point of strong discussion, Meanwhile best practices exist, e.g. VALIKOM or MySkills from Germany, the broad adoption of these methods cannot answer all critiques raised from firms and assessment practitioners. Specifically, among educational providers the question remains, whether short assessments are a suitable form of replacing an entire formation curriculum. To increase the validity of the measurement process, several points need to be taken into account:

1. Transparent processes. The transparency of the entire recognition process is key. An intake discussion, an assignment of a dedicated mentor and the proper preparation for the assessment need to be included in a holistically thought out, step-by-step planned recognition process.

2. The recognition itself needs to take into account several measures in order to ensure the highest possible validity of the assessment. Generally, specific forms of assessments are more suited to assess specific forms of competences. Meanwhile written tests, be it with open answers or multiple choice, are suitable to assess knowledge, role plays, post box exercises or pitch presentation gaming are geared for testing communicative and social competences like interviewing, rhetoric, argumentation, empathy, assertiveness, persuasiveness, sensitivity (behavioral observation). They are also useful for assessing operational readiness, goal orientation, frustration tolerance, persistence, problem solving skills, analytic skills, decision making skills etc. Biographical methods like criterion based interviews, review of a structured portfolio and technical discussions candidates gain comprehensive insight into their own achievements and learn to assess themselves and their qualities. Finally, observations on sight and in a simulated environment allow for the observation of reactions in real life scenarios, self-conduct and approach to spontaneous events. Therefore, by a mixture of assessment methods, granular competences can be triangulated and the disposition reliable determined.

3. In order to conduct objective assessments, assessors need to be trained to deal with different assessment methods, different assessment biases and different candidates in a fair, transparent and objective manner. The assessors need to be aware of the different learning biographies and different objectives of the candidates and understand the entire validation and recognition process.

4. Self-assessments as a step towards the assessment are recommended, but self-assessment as a source of assessment are not recommended. Self-assessments either in the form of technical assessments (“candidate X knows…” “Yes”, “no”) or in the form of personality tests can yield indicative results, however the reliability and objectivity of these results are to be questioned.

Therefore, a detailed structure and quality assurance system needs to be put into place to guarantee the reliable, objective and transparent assessment and to create trust among educational institutions and employers.

4 Outlook & Recommendations

The shortage of skilled labour in the sector of information security remains persistent across the EU. Technical competences among professionals face increasing irrelevance in comparison to social and personal competences. Investments into human capital, i.e. proper education for employees, are increasingly more profitable in the face of diffuse risk situations such multidimensional attack vectors in the physical and digital space. The security of a firms know-how and readiness of internal and external services is increasingly coupled with new exploitation potentials. But in the end, all new technologies and guidelines introduced to curb the risk of hostile breaches are nullified of the companies employees don't consent to and actively life the firms security culture.

Awareness of risks and adherence to policies are the starting point to diminish risks for any sort of attacks. To achieve this, values, beliefs and ultimately behavior of the people in a firm need to be changed with the end to establish a vital risk culture. The shift of attention away from the technical end of the underlying problem towards the human factor makes it clear that education and training need to thought from this angle as well.

The increased criminal activity in relation to private and confidential information in the digital age poses questions not only to the formation of capabilities in professional environments and the working domain, but also to the private sphere of European citizens. Even though attacks against corporations cause significant damage to the European economy, it is important to highlight the ramifications of increased criminal activity in context of confidential information: it targets individuals, not firms. Consequently, building capabilities among citizens through primary education and training would create positive externalities for businesses and the society. Capacity building should therefore not only be considered to be the interest of individual firms – but of the general public. The introduction of awareness training, conduct of sensitive information and understanding of the own exposure to hostile attacks in schools, vocational and higher educational institutions. In 2018, the Council of the European Union redefined "Civic Competence" as

"the ability to act as responsible citizens and participate fully in civic and social life, based on an understanding of social, economic, legal and political concepts and structures, as well as global developments and sustainability".

The participation as mature citizens in the world of today and tomorrow is closely tied to the ability of separating intentional harm from every day incidents. Detecting misinformation, manipulation, cherishing privacy and digital security are a question of civic resilience – and should not be constricted to a question of profitable spending in private corporations. Ultimately, it is in the best interest of the European Union and its member states – and therefore a question to be answered by education ministries – not only IT-departments.

As a consequence, the following means are recommended to built capabilities among European citizens:

1. Founding of a European Organization for the protection of private information and data. Implementing a point of contact, an arena for shared beliefs in a critical matter and a platform for knowledge exchange and interest campaigning is a crucial part to steer civic, public and corporate interest. The main objective, the promotion of the remaining recommendations enlisted below, lie at the heart of a common organization.
2. Introducing “Information Security” in apprenticeship curricula ceteris paribus “health and safety”. It is economically unfeasible to change human values, beliefs and actions. Therefore, it is important to engage in the formation process, and to teach individuals the importance of awareness towards diffuse threat scenarios, including targeted manipulation and misinformation in the digital age.
3. Introducing Micro-Credentials and partial certification schemes for Information Security for private and professional reception. The current situation in continuing education and training remains intransparent and lacks a structured vision towards the future. Next to existing certification schemes, fully fledged curricula, built up by singular and trainable modules, provide manifold opportunities for usage and replication. They can be integrated into VET training (EQF 4) and higher education (EQF 6-7) according to the subject, combined into a singular training path which connects work-based training and higher education (EQF5), or, be offered to employees as continuing education opportunities. The modularization allows for a targeted and less complex and resource intensive training pattern, yielding lower costs and greater opportunities for SMEs.
4. Increase the usage of European transparency tools to support flexibility on the labor market and attract new talent.

5 Literature

Andrea Antonelli (2020): Il GDPR in Italia due anni dopo: a che punto siamo? Online verfügbar unter https://blog.osservatori.net/it_it/gdpr-in-italia-stato-adeguamento, zuletzt geprüft am 10.08.2021.

Austrian Press Agency (2020): EU-DSGVO: Verständnis ja, Umsetzung schleppend. KSV1870 Unternehmenskommunikation. Wien (OTS0017). Online verfügbar unter https://www.ots.at/presseaussendung/OTS_20200519_OTS0017/eu-dsgvo-verstaendnis-ja-umsetzung-schleppend, zuletzt aktualisiert am 14.07.2021, zuletzt geprüft am 14.07.2021.

Bitkom e.V. (2020): Studie: Datenschutzverordnung & Privacy Shield. Online verfügbar unter https://www.bitkom.org/sites/default/files/file/import/Studie-Datenschutzgrundverordnung.pdf, zuletzt geprüft am 22.07.2021.

BVerfG (15.12.1983): Volkszählungsurteil. 1 BvR 209/83.

Cedefop (2009): European qualifications framework (EQF). Online verfügbar unter https://www.cedefop.europa.eu/en/events-and-projects/projects/european-qualifications-framework-eqf, zuletzt aktualisiert am 17.06.2021, zuletzt geprüft am 05.07.2021.

datenschutz (2021): EU-Datenschutzgrundverordnung I Datenschutz 2021. Online verfügbar unter https://www.datenschutz.org/eu-datenschutzgrundverordnung/, zuletzt geprüft am 28.07.2021.

Deloitte Services Wirtschaftsprüfungs GmbH (2020): Deloitte Umfrage Bestandsaufnahme nach 18 Monaten EU-DSGVO, 2020. Online verfügbar unter https://www2.deloitte.com/content/dam/Deloitte/at/Documents/risk/at-eu-dsgvo-umfrage-2020.pdf, zuletzt geprüft am 27.07.2021.

EUR-LEX: NIS Directive (EU) 2016/1148. Online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32016L1148, zuletzt geprüft am 27.07.2021.

EUR-LEX (1995): Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A31995L0046, zuletzt geprüft am 27.07.2021.

European Commission (Hg.) (2008): Explaining the European Qualifications Framework for Lifelong Learning. Office for Official Publications of the European Communities. Luxembourg. Online verfügbar unter https://europa.eu/europass/system/files/2020-05/EQF-Archives-EN.pdf, zuletzt geprüft am 05.07.2021.

European Commission (2020a): COM/2020/66 final. A European strategy for data. Brussels.

European Commission (02.06.2020): Commission launches consultation to seek views on Digital Services. Online verfügbar unter https://ec.europa.eu/commission/presscorner/detail/en/ip_20_962.

European Commission (2020b): COM/2020/264 final. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation. Brussels.

Eurostat (2021): Purchasing power adjusted GDP per capita. Online verfügbar unter https://ec.europa.eu/eurostat/databrowser/view/sdg_10_10/default/table?lang=en, zuletzt geprüft am 23.07.2021.

Federal Ministry of Finance (BMF): Data Protection. Online verfügbar unter https://www.bmf.gv.at/en/data-protection.html, zuletzt geprüft am 27.07.2021.

GDPD (2020): Relazione annuale 2020. Online verfügbar unter https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9676435, zuletzt geprüft am 10.08.2021.

heyData (2021): Europa im Datenschutz-Ranking. Online verfügbar unter https://www.heydata.eu/europa-im-datenschutz-ranking, zuletzt aktualisiert am 22.07.2021, zuletzt geprüft am 22.07.2021.

KSV1870: DSGVO-Assistent. Online verfügbar unter https://www.ksv.at/spezielle-loesungen/dsgvo-assistent, zuletzt geprüft am 14.07.2021.

Lienhardt, Conrad (2020): Informationspflicht nach DSGVO. Online verfügbar unter https://fokus.genba.org/informationspflichten-dsgvo, zuletzt aktualisiert am 20.02.2020, zuletzt geprüft am 14.07.2021.

May, Sandra (2021): Deutschland ist Europa-Meister in Sachen Datenschutzverstöße. In: *OnlinehändlerNews*, 29.06.2021. Online verfügbar unter https://www.onlinehaendler-news.de/e-recht/gesetze/134980-deutschland-europa-titel-datenschutzverstoesse, zuletzt geprüft am 23.07.2021.

Office for Personal Data Protection (2018): Personal Data Protection at the Workplace. Guidebook for Employers. Warsaw. Online verfügbar unter https://uodo.gov.pl/pl/file/1469.

Rechtsinformationssystem des Bundes (RIS) (1999): Federal Act concerning the Protection of Personal Data (DSG). Online verfügbar unter https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Erv&Dokumentnummer=ERV_1999_1_165, zuletzt aktualisiert am 26.02.2020, zuletzt geprüft am 27.07.2021.

Simon, Herbert A. (1990): Bounded Rationality. In: John Eatwell, Murray Milgate und Peter Newman (Hg.): Utility and probability. London: Macmillan reference Books (The new palgrave), S. 15–18.

Statista (2020): Wie weit sind Sie mit der Umsetzung der Datenschutz-Grundverordnung? Online verfügbar unter https://de.statista.com/statistik/daten/studie/917518/umfrage/stand-der-umsetzung-der-dsgvo-durch-unternehmen-in-deutschland/, zuletzt geprüft am 28.07.2021.

Tessian (2021): The Psychology of Human Error | Tessian. Online verfügbar unter https://www.tessian.com/research/the-psychology-of-human-error/, zuletzt aktualisiert am 24.02.2021, zuletzt geprüft am 06.07.2021.

Wirtschaftskammer Österreich (2020): IT-Sicherheit, Datensicherheit. Wien. Online verfügbar unter https://www.wko.at/service/innovation-technologie-digitalisierung/it-sicherheit-datensicherheit.html, zuletzt geprüft am 14.07.2021.

Wirtschaftskammer Österreich (2021a): IT Safe. Wien. Online verfügbar unter https://www.wko.at/site/it-safe/start.html, zuletzt geprüft am 14.07.2021.

Wirtschaftskammer Österreich (2021b): EU-Datenschutz-Grundverordnung (DSGVO). Überblick zum Datenschutz in Österreich. Wien. Online verfügbar unter https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung.html, zuletzt geprüft am 14.07.2021.

ZFODO (2020): The 10 biggest mistakes in ensuring compliance with RODO. Warsaw. Online verfügbar unter https://www.zfodo.org.pl/wp-content/uploads/2020/05/10-najwiekszych-bledow-przy-wdrazaniu-RODO.pdf.

ZFODO (2021): Breaches in personal data protection 2020. Warsaw. Online verfügbar unter https://www.zfodo.org.pl/wp-content/uploads/2020/11/Breach-report-2020-ZFODO.pdf, zuletzt geprüft am 07.07.2021.

Strategic Report

We thank the co-authors and from:

BF/M-Bayreuth

Mykolas Romeris University

WSBiNoZ

Consulenza Direzionale di Paolo Zaramella

Hafelekar Unternehmensberatung

Teilzertifizierung im Berufsfeld Informationssicherheit - TeBeISi

Funded by the Erasmus+ Programme of the European Union

https://information-security-in-sme.eu/.