National Adaption Plan

Considering the gaps – national institutional playing fields and strategic partnerships

Funded by the Erasmus+ Programme of the European Union

TeBelSi

Funded by the
Erasmus+ Programme
of the European Union

This document is licensed under CC BY-SA 4.0.

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

The European Commission support for the production of this publication does not constitute endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Content

List of Figures

List of Tables

1 Introduction

The project “Partial Certification in the professional field of Information Security” is considering not only recent developments in information security, but also in education and training. Looking at these fields on a European scale, it becomes quite clear that the projects outcome will have to take a wide range of facets into account in order to provide a solution which is not only feasible for an individual or a firm in one country, but which can be looked at from a European perspective.

Considering the former, the economies among the member states differ vastly in terms of predominant industry branches, formalization of legal requirements and spread of personal or organizational certification requirements. These differences grow when comparing the educational ramifications – especially the vocational education and training (VET) organisation. In consequence, new perspectives on learning and the consideration of a Europeanised credit transfer systems (ECVET) provide the foundation of how the project suggests to facilitate SMEs across the EU to built up own information security capabilities. The solution suggested in this project – self-evaluation in combination with units for micro-learning- are based on the different ramifications and status-quo existing in the member countries of this project.

Due to the opaqueness if the projects subject, manifold stakeholders need to be considered and integrated into the strategic development of the project adaption. To this end, the project partners conducted stakeholder analyses and formed a steering group committee in each member state, which was consulted to gain insight perspectives from educational institutions, SMEs, information security practitioners and associations active in the field of information security.

Consequently, this document is structured as follows: Chapter 2 provides a background of information security and information security education in each partner country, Chapter 3 sets out key conclusions and derives the strategy to tackle the underlying problem of this project. Chapter 4 illustrates feedback collected from the steering group and discusses the findings and proposals in terms of their feasibility. Finally, chapter 5 concludes the national adaption plan and sets out the next steps.

2 Background Information (All partners) (Summary)

2.1 Germany

2.1.1 Legal Environment of Information Security in Germany

Information security is not specifically regulated by law in Germany. However, the necessity to provide for information security measures arise from a series of legislation, both from the areas of corporate governance and information and IT security. In contrast, data protection underlies strict regulatory premises.

Corporate Governance

In the past years several legal regulations were passed, from which direct action and liability obligations of the executive board or more specifically the management of a company to questions about information security can be deducted. Those regulations apply both for stock companies as well as limited liability companies.

Principles of the Corporate Governance were codified in the German Corporate Governance Code. Next to essential legal regulations about corporate management and publicity the code provides information about recommendation to the direcitng and monitoring of publicly traded companies.

In this context it is pointet to the law of control and transparency in business units (“Gesetz zur Kontrolle und Transparenz im Unternehmensbereich”, KonTraG), which became effective in May 1998. The KonTraG is a so-called articel law and complements or changes laws like the commercial code (“Handelsgesetzbuch”, HGB) and the Stock Corporation Act (“Aktiengesetz”). In particular, the demand for an early risk detection system for corporations – that means for stock corporations and limited liability companies – was not included in the previous regulations and had to be set up by the companies themselves. As part of the European measure EuroSox in 2006, minimum requirements for risk management were described and the duties of auditors were defined. In Germany, the Accounting Modernisation Act (“Bilanzierungsmodernisierungsgesetz”, BilMoG) came into force in 2012, which requires corporations, for example, to present their internal control systems in annual financial statements.

The managing directors of a limited liability company (in German GmbH) are required by the **GmbH-regulations** to exercise "the diligence of a prudent businessman" (§ 43 Abs. 1 GmbHG). Issues of consumer protection are dealt with in various laws. The use of information technology, the use of the internet or the use of telecommunications services are regulated very precisely. Relevant laws include, for example, the law on the use of teleservices (“Gesetz zur Nutzung von Telediensten”), the Telecommunications Act (“Telekommunikationsgesetz”), the State Treaty on Media

Services (“Mediendienste-Staatsvertrag”), copyright law (“Urheberrecht”) as well as various directives at EU level. The handling of personal data is regulated in the data protection laws of the federal and state governments (“Datenschutzgesetzen des Bundes und der Länder”), the law on data protection for teleservices, the Telecommunications Data Protection Ordinance (“Telekommunikations-Datenschutzverordnung”) and in some cases in the laws already listed (BSI 2012, p. 17f.)(Bundesamt für Sicherheit in der Informationstechnik 2012, p. 17f.).

In the HGB, due diligence is imposed in Section 347. Generally speaking, "diligence" is measured differently from industry to industry. However, the same standard applies everywhere: a businessman (definition of a businessman according to section 1 HGB) is obliged to inform himself about the corresponding rules of his commercial business. It can therefore be deduced that a businessman must constantly inform himself independently about current norms and laws and must be liable for the damage incurred in the event of non-compliance. Nevertheless, this is not explicitly codified, but is regarded as a general standard on which entrepreneurial action is based.

It is therefore of existential importance for companies to understand IT security as part of their entrepreneurial duty of care. Knowledge of the aforementioned legal content and the significance of the underlying standards of due diligence are therefore essential for the correct handling of data protection and information security.

Information Security

The law to increase the security of information technology systems (“Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme”, IT Security Act (IT-SiG)), which came into force in July 2015, is an article law which amends and supplements the law of the Federal Office for Information Security (“Bundesamtes für Sicherheit in der Informationstechnik”, BSI), the Energy Industry Act (“Energiewirtschaftsgesetz“), the Telemedia Act (“Telemediengesetz”) and the Telecommunications Act (“Telekommunikationsgesetz”). The IT-SiG represents a revised version of the federal act to strengthen security in information technology of the federal government of 2009 and is intended to meet the needs of the changing risk situation through the progressing digitalisation of state, economy and society. At the same time, the "IT Security Catalogue pursuant to Section 11 (1a) EnWG" was adopted, which establishes IT security requirements specifically for operators of electricity and gas grids. A further security catalogue ("IT security catalogue pursuant to Section § 11 paragraph 1b EnWG") was published in December 2018, in which the security requirements for operators of energy systems are defined.

The law was extended in May 2016 by the KRITIS regulation, the first part of the BSI ordinance. The June 2017 amendment stipulated that the energy, water, transport and traffic, health, finance and insurance sectors are to be classified as Critical Infrastructures (KRITIS) and are therefore obliged to equip their IT systems with state-of-the-art technology and have their information security checked every two years. Since May 2018, the Basic Data Protection Regulation

(“Datenschutzgrundverordnung”, DSGVO) issued by the European Commission has provided these standards for other companies with sensitive data (Bundesnetzagentur 2019).

Based on the federal government's digital agenda from 2014, the law is intended to contribute to improving the security and protection of IT systems and services. Particularly with regard to critical infrastructures, threats or supply bottlenecks would have far-reaching consequences for the state, the economy and society in Germany. The KRITIS Ordinance (BSI-KritisV) clarifies which facilities, installations or parts thereof are specifically covered by the requirements of the IT-SiG. Further goals of the law are an improved IT security of enterprises, administration, institutions as well as a larger protection of Federal citizens for the use of the Internet. The main adressees are operators of critical infrastructures, web service providers, telecommunications companies and the BSI (BSI 2016).Based on the federal government's digital agenda from 2014, the law is intended to contribute to improving the security and protection of IT systems and services. Particularly with regard to critical infrastructures, threats or supply bottlenecks would have far-reaching consequences for the state, the economy and society in Germany. The KRITIS Ordinance (BSI-KritisV) clarifies which facilities, installations or parts thereof are specifically covered by the requirements of the IT-SiG. Further goals of the law are an improved IT security of enterprises, administration, institutions as well as a larger protection of Federal citizens for the use of the Internet. The main adressees are operators of critical infrastructures, web service providers, telecommunications companies and the BSI (BSI 2016, S. 5).

In June 2017, the directive on high network and information security (NIS Directive) was issued by the European Commission in order to create a uniform legal framework to strengthen IT security for KRITIS operators and providers of digital services. In terms of content, the IT-SiG covers the obligations of critical infrastructures, which was extended in May 2018 to include the law enacted to implement the NIS Directive (BSI 2019).In June 2017, the directive on high network and information security (NIS Directive) was issued by the European Commission in order to create a uniform legal framework to strengthen IT security for KRITIS operators and providers of digital services. In terms of content, the IT-SiG covers the obligations of critical infrastructures, which was extended in May 2018 to include the law enacted to implement the NIS Directive (BSI 2019).

In practice, standards have been developed by the BSI to ensure that companies meet information security requirements. The BSI standards define requirements for an information security management system (BSI Standard 200-1), which is intended to ensure that personal data is processed in compliance with the law. Standard 200-1 conforms to the international standard ISO 27001 (Bundesnetzagentur 2015).In practice, standards have been developed by the BSI to ensure that companies meet information security requirements. The BSI standards define requirements for an information security management system (BSI Standard 200-1), which is intended to ensure that personal data is processed in compliance with the law. Standard 200-1 conforms to the international standard ISO 27001 (Bundesnetzagentur 2015).

With the changing legal situation and the associated classification of energy plants as critical infrastructures, there are new requirements for the IT security of the affected companies, which have until the end of February 2019 to name their contact person for IT security to the Federal Network Agency and subsequently have to provide proof by 31 March 2021 that the requirements of the security catalogue have been implemented. Knowledge of the new requirements is therefore of vital importance both for the companies and for the employees responsible for information security. An information security management system (ISMS) for SMEs is not (yet) legally binding. In practice, however, it is necessary to comply with standards in the supply chain when doing business with listed companies, as this is required in the supply contracts.

Data Protection

The Basic Data Protection Ordinance (DSGVO), which came into force in May 2018, replaces the Federal Data Protection Act ("Bundesdatenschutzgesetz", BDSG-alt) in Germany, which had been in force until then. The implementation of the opening clauses contained in the DSGVO was regulated in Germany by the EU Data Protection Adaptation and Implementation Act (BDSG-new), which became effective at the same time and thus supplements the DSGVO with the leeway given to the federal states. In addition, the BDSG-new also regulates areas that remain unaffected by the DSGVO (Datenschutz.org 2018).The Basic Data Protection Ordinance (DSGVO), which came into force in May 2018, replaces the Federal Data Protection Act ("Bundesdatenschutzgesetz", BDSG-alt) in Germany, which had been in force until then. The implementation of the opening clauses contained in the DSGVO was regulated in Germany by the EU Data Protection Adaptation and Implementation Act (BDSG-new), which became effective at the same time and thus supplements the DSGVO with the leeway given to the federal states. In addition, the BDSG-new also regulates areas that remain unaffected by the DSGVO (Datenschutz.org 2018).The Basic Data Protection Ordinance (DSGVO), which came into force in May 2018, replaces the Federal Data Protection Act ("Bundesdatenschutzgesetz", BDSG-alt) in Germany, which had been in force until then. The implementation of the opening clauses contained in the DSGVO was regulated in Germany by the EU Data Protection Adaptation and Implementation Act (BDSG-new), which became effective at the same time and thus supplements the DSGVO with the leeway given to the federal states. In addition, the BDSG-new also regulates areas that remain unaffected by the DSGVO (Datenschutz.org 2018).The Basic Data Protection Ordinance (DSGVO), which came into force in May 2018, replaces the Federal Data Protection Act ("Bundesdatenschutzgesetz", BDSG-alt) in Germany, which had been in force until then. The implementation of the opening clauses contained in the DSGVO was regulated in Germany by the EU Data Protection Adaptation and Implementation Act (BDSG-new), which became effective at the same time and thus supplements the DSGVO with the leeway given to the federal states. In addition, the BDSG-new also regulates areas that remain unaffected by the DSGVO (Datenschutz.org 2018).

The new BDSG is divided into four sections: The first part contains general provisions, the second part deals with the specification and amendment of the DSGVO, part 3 implements the EU Data Protection Directive for Police and Justice (EU 2016/680) (and therefore does not apply to private companies) and part 4 regulates areas that are neither covered by the DSGVO nor by Directive 2016/680 (Datenschutz.org 2018).The new BDSG is divided into four sections: The first part contains general provisions, the second part deals with the specification and amendment of the DSGVO, part 3 implements the EU Data Protection Directive for Police and Justice (EU 2016/680) (and therefore does not apply to private companies) and part 4 regulates areas that are neither covered by the DSGVO nor by Directive 2016/680 (Datenschutz.org 2018).The new BDSG is divided into four sections: The first part contains general provisions, the second part deals with the specification and amendment of the DSGVO, part 3 implements the EU Data Protection Directive for Police and Justice (EU 2016/680) (and therefore does not apply to private companies) and part 4 regulates areas that are neither covered by the DSGVO nor by Directive 2016/680 (Datenschutz.org 2018).The new BDSG is divided into four sections: The first part contains general provisions, the second part deals with the specification and amendment of the DSGVO, part 3 implements the EU Data Protection Directive for Police and Justice (EU 2016/680) (and therefore does not apply to private companies) and part 4 regulates areas that are neither covered by the DSGVO nor by Directive 2016/680 (Datenschutz.org 2018).

The complementary character of the BDSG-new can be seen in various places. Article 38, together with the DSGVO, regulates, among other things, when a data protection officer must be appointed (This is the case if the processing by a private position involves extensive or systematic observation of persons, if the core activity of the position is the processing of personal data, if at least ten persons are permanently engaged in the automated processing of personal data and (irrespective of the number of persons entrusted) if data are processed for the purpose of transmission of market and opinion research) (Landesbeauftragte für Datenschutz und Informationssicherheit Nordrhein-Westfalen 2019). Another point is the employment data protection (DSGVO Art. 88), which explicitly provides for national regulations. This was implemented by § 26 BDSG-neu. Finally, the BDGS provides for punitive measures in the event of data protection violations (§ 42), which go beyond the envisaged fines of the DSGVO (Art. 83). The complementary character of the BDSG-new can be seen in various places. Article 38, together with the DSGVO, regulates, among other things, when a data protection officer must be appointed (This is the case if the processing by a private position involves extensive or systematic observation of persons, if the core activity of the position is the processing of personal data, if at least ten persons are permanently engaged in the automated processing of personal data and (irrespective of the number of persons entrusted) if data are processed for the purpose of transmission of market and opinion research) (Landesbeauftragte für Datenschutz und Informationssicherheit Nordrhein-Westfalen 2019). Another point is the employment data protection (DSGVO Art. 88), which explicitly provides for national regulations. This was implemented by § 26 BDSG-neu. Finally, the BDGS provides for punitive measures in the event of data

protection violations (§ 42), which go beyond the envisaged fines of the GDPR (Art. 83). The complementary character of the BDSG-new can be seen in various places. Article 38, together with the DSGVO, regulates, among other things, when a data protection officer must be appointed (This is the case if the processing by a private position involves extensive or systematic observation of persons, if the core activity of the position is the processing of personal data, if at least ten persons are permanently engaged in the automated processing of personal data and (irrespective of the number of persons entrusted) if data are processed for the purpose of transmission of market and opinion research) (Landesbeauftragte für Datenschutz und Informationssicherheit Nordrhein-Westfalen 2019). Another point is the employment data protection (DSGVO Art. 88), which explicitly provides for national regulations. This was implemented by § 26 BDSG-neu. Finally, the BDGS provides for punitive measures in the event of data protection violations (§ 42), which go beyond the envisaged fines of the DSGVO (Art. 83). The complementary character of the BDSG-new can be seen in various places. Article 38, together with the DSGVO, regulates, among other things, when a data protection officer must be appointed (This is the case if the processing by a private position involves extensive or systematic observation of persons, if the core activity of the position is the processing of personal data, if at least ten persons are permanently engaged in the automated processing of personal data and (irrespective of the number of persons entrusted) if data are processed for the purpose of transmission of market and opinion research) (Landesbeauftragte für Datenschutz und Informationssicherheit Nordrhein-Westfalen 2019). Another point is the employment data protection (DSGVO Art. 88), which explicitly provides for national regulations. This was implemented by § 26 BDSG-neu. Finally, the BDGS provides for punitive measures in the event of data protection violations (§ 42), which go beyond the envisaged fines of the DSGVO (Art. 83).

These are only a few examples of the interaction between the Federal Data Protection Act and the Basic Data Protection Ordinance. In principle, when applying the DSGVO, attention must be paid to statements in the BDSG (Datenschutz.org 2018).These are only a few examples of the interaction between the Federal Data Protection Act and the Basic Data Protection Ordinance. In principle, when applying the DSGVO, attention must be paid to statements in the BDSG (Datenschutz.org 2018).These are only a few examples of the interaction between the Federal Data Protection Act and the Basic Data Protection Ordinance. In principle, when applying the DSGVO, attention must be paid to statements in the BDSG (Datenschutz.org 2018).These are only a few examples of the interaction between the Federal Data Protection Act and the Basic Data Protection Ordinance. In principle, when applying the DSGVO, attention must be paid to statements in the BDSG (Datenschutz.org 2018).

Security officers are required to have precise knowledge of data protection law following the amendment in 2018. All in all, the laws introduced in recent years place high demands on the correct handling of information and data security, which makes continuous further training of security officers in legal issues indispensable. This poses particular challenges for small and medium-sized enterprises (SMEs), as the resources

required for this, such as their own IT or legal advice, are not sufficient for this type of conversion processes.

Conclusion

In summary, the ISO 27001, where the requirements for an Information Security Management System (ISMS) of a company are defined, is the most important reference for the establishment of information security in corporations and public bodies. In addition to ISO 27001 the German baseline protection standards exist. These standards provide comprehensive instructions on how to implement and maintain a security concept based on standard security measures formulated in detail. Among others, the standard is recommended by the Federal Commissioner for Data Protection in Germany (BSI 2012).

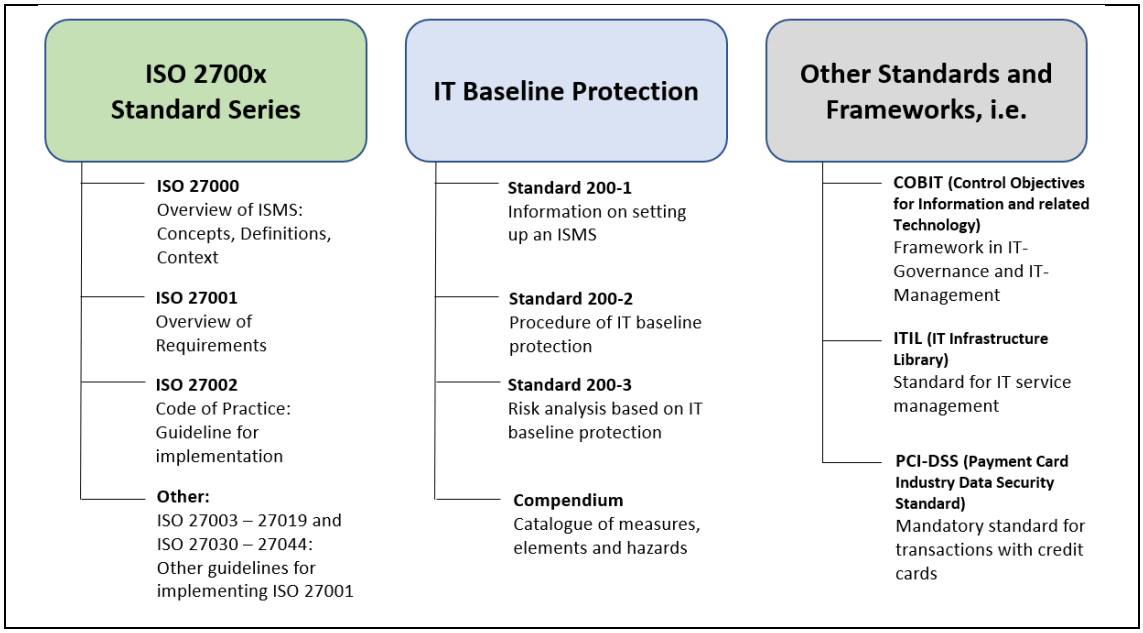

Figure 1: Standards in the Field of Information Security.
Source: Own illustration.

Other standards regarding information security are the IT governance framework COBIT, the standard for IT service management ITIL or PCI-DSS as a mandatory standard for the security of credit card transactions. Figure 1 shows the most important standards in Germany. Companies will have also the opportunity to get a certification for most standards if they are compliant to the requirements. This can be useful to fulfil external requirements, such as demands from customers, which in Germany are commonly acquired, e.g. by the automobile industry. A reason for firms to obtain such certifications arises from the general structure of the economy, as many SMEs operate as suppliers to larger corporations.

The external demand or the desire to signal certain competences in the field of information security represent strong motivational aspects for the implementation of security system, despite the absence of legal obligations (Kersten et al. 2013).

Compliance with these legal requirements, as well as the implementation of a complex security concept based on standards is associated with a high level of effort and requires qualified personnel - especially for SMEs a challenging situation. These companies are often dependent on external support. Thus, the application of the ISO 27001 series is rather unsuitable for SMEs due to its complexity in combination with missing of know-how, high effort and costs (Barlette und Fomin 2008)The external demand or the desire to signal certain competences in the field of information security represent strong motivational aspects for the implementation of security system, despite the absence of legal obligations (Kersten et al. 2013). Compliance with these legal requirements, as well as the implementation of a complex security concept based on standards is associated with a high level of effort and requires qualified personnel - especially for SMEs a challenging situation. These companies are often dependent on external support. Thus, the application of the ISO 27001 series is rather unsuitable for SMEs due to its complexity in combination with missing of know-how, high effort and costs (Barlette und Fomin 2008).

2.1.2 Information Security Education and Training in Germany

The German education system inherits a dual approach to academic and vocational training, the dual system. Meanwhile, after completing a lower-secondary education course (i.e. school) learners have the possibility to enter either a vocational training or an academic course, depending on their qualification. Meanwhile the former leads to qualifications on the levels from 6-8, the latter yields a qualification on the levels 3-4, with further qualification possibilities via continuing education, leading up to qualification possibilities at EQF level 8. However, it needs to be highlighted that the defined EQF level 5 is atypical in many partner countries. In the following, an overview of students enrolled in courses on EQF level 5-8 in Germany illustrates this speciality in comparison other EU countries. So called “short circle tertiary education programs” are mostly common in France, Spain and the UK (Eurostat 2020b).

	Germany		Austria		Lithuania		Italy		Poland	
EQF	number	% share	number	% share	num-ber	% share	number	% share	number	% share
5	349	0,01%	75.217	17,48%	-	-	13.378	0,71%	234	0,02%
6	1.872.666	59,87%	199.236	46,31%	88.468	74,79%	1.140.641	60,16%	986.723	66,09%
7	1.054.512	33,71%	135.346	31,46%	27.076	22,89%	713.633	37,64%	464.624	31,12%
8	200.400	6,41%	20.396	4,74%	2.743	2,32%	28.338	1,49%	41.318	2,77%
To-tal	3.127.927	100,00 %	430.195	100,00 %	118.287	100,00 %	1.895.990	100,00 %	1.492.899	100,00%

Table 1: Amount of EQF 5 qualifications issued among the partner states
Source: (Eurostat 2020a).

http://ec.europa.eu/eurostat/web/education-and-training/data/database

The German education system inherits a dual approach to academic and vocational training, the dual system. Meanwhile, after completing a lower-secondary education course (i.e. school) learners have the possibility to enter either a vocational training or

an academic course, depending on their qualification. Meanwhile the former leads to qualifications on the levels from 6-8, the latter yields a qualification on the levels 3-4, with further qualification possibilities via continuing education, leading up to qualification possibilities at EQF level 8. However, it needs to be highlighted that the defined EQF level 5 is atypical in many partner countries. In the following, an overview of students enrolled in courses on EQF level 5-8 in Germany illustrates this speciality in comparison other EU countries. So called “short circle tertiary education programs” are mostly common in France, Spain and the UK (Eurostat 2020b).

Concerning educational institutions, the availability of courses and certificates is very diverse. In general, there are four categories of educational providers which offer certificates or courses of any kind: Courses leading to a qualification including 1) VET providers (EQF 3-5) and 2) Higher Education (HE) (EQF 6-8) as well as courses leading to certificates (unregulated and regulated) by either 3) private certification providers or 4) continuing education providers (c.f. Annex I to this document for an overview of existing training courses on the various EQF levels).

It can be noted that in terms of formal qualifications, numerous offerings exist regarding related fields in cyber security and IT security on a university level. However, new curricula with a focus on law in information technology are on the rise. Meanwhile VET providers, especially the chambers of commerce, offer continuing training courses after the initial 3-3.5 years training, which allow for training of subdomains in the IT field, the IT Security Technician and IT Security Coordinator aim to take needs of SMEs into account. In 2020, the 4 existing profiles have been reorganised. The new descriptions of the occupational profile are included in the table below.

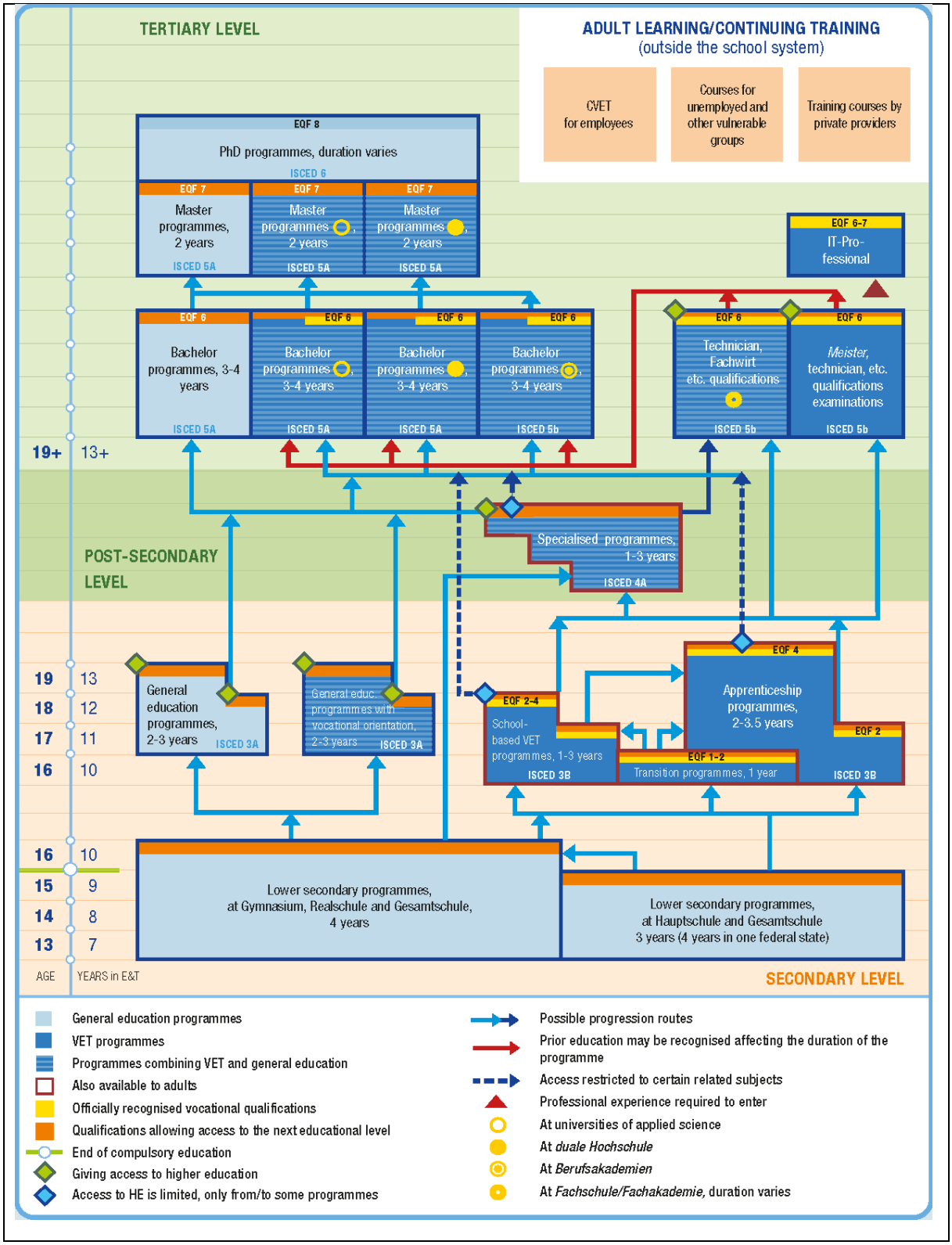

Figure 2: The German Education System
Source: (Cedefop 2014).

Concerning the existence of two courses concerning IT Security, it can be inferred from the numbers above that only a small proportion of learners is taking advantage of these education possibilities.

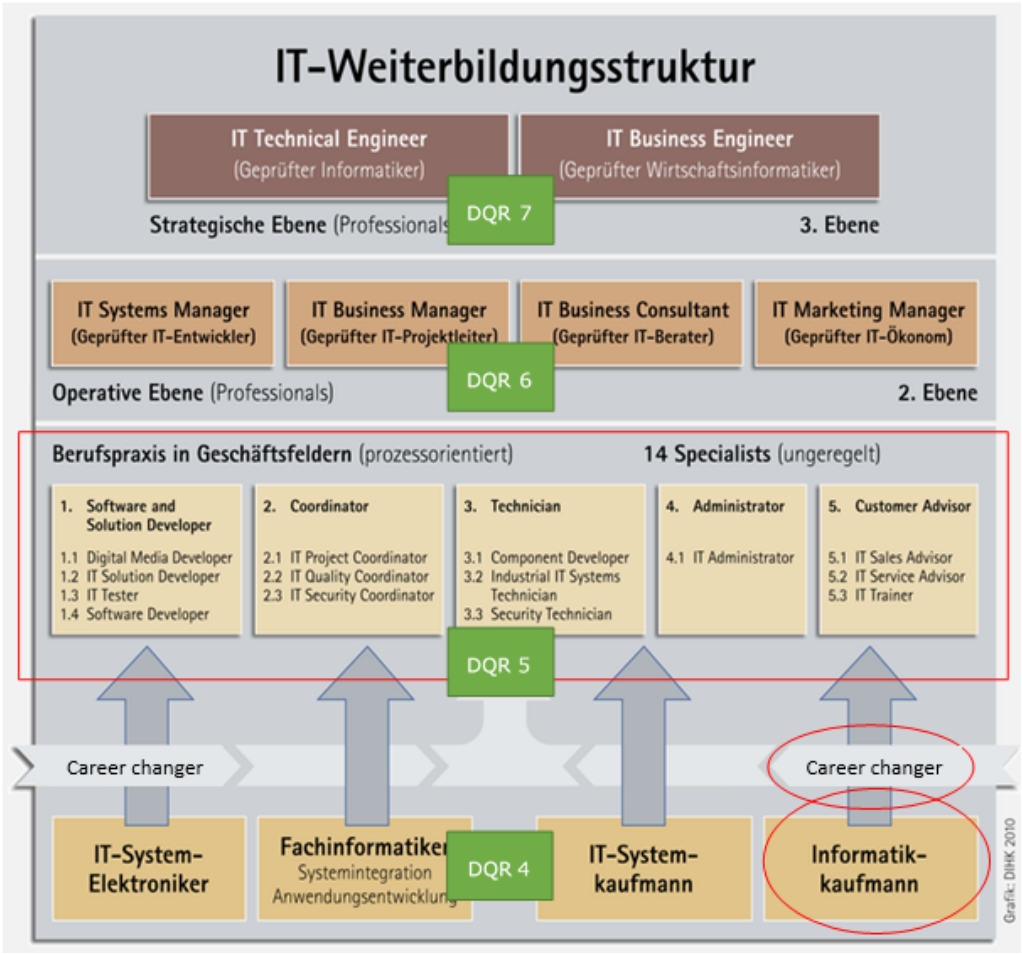

Figure 3: Continuing Training Structure of the IHK
Source: Own illustration based on IHK (2018)

In Appendix I to this document, examples of courses from each category with a close relation to information security shall be provided:

1) Vocational Education and Training possibilities
2) Higher Education Possibilities
3) Private Certification Providers (Personnel certification) for Information Security and Data Protection.

2.1.3 Information Security Labour Market in Germany

The situation on the labour market for qualified personnel in the field of information security remains tense. There are hardly any IT specialists on the job market right now and those who are available are in high demand. Usually, smaller companies cannot pay the respective high salaries which are offered by larger corporations.

There are several reasons which lead to the current situation, and which should be considered when thinking about solutions. First, the lack of qualified personnel goes hand in hand with increasing requirements concerning knowledge and skills posed by several directives and regulations on national and international level. Second, companies didn't recognize in time the future need of qualified personnel and did not engage early enough in education and training activities of own resources. Finally, the increasing ease of orchestrating attacks and inflicting damage via a marketization of exploits resulted in a rapid growth of hostile actions and tools available, yielding a fast upcoming of information security incidents and surprising many firms on the market.

An interesting point regarding qualifications and competencies in the context of lacking qualified personnel is that a university degree is generally not perceived a basic requirement in the field of information security (which is also true in the IT sector in general). Especially in the technical skills domain a completed vocational training combined with work experience is worth the same as a university degree. In general, however, firms want to see that the applicant has obtained some sort of educational qualification.

2.2 Institutional Landscape

For a concise overview of relevant actors, see Annex II to this document.

2.3 Stakeholder Analysis

In Germany, actors from several domains exist which follow institutionalised and long-term patterns of actions. Stakeholders exist with a focus on education and training (mainly the Chambers of Commerce), Higher Education (Universities), organizations concerned with Information Security and Data Protection in general (mainly private initiatives), further qualification (private education providers) as well as certification providers.

The field of actors can be described as generally heterogeneous, however some actors are more important then others to the project. First, some organizations are specifically concerned with the needs of SMEs and have an inherent motivation to provide solutions designed around the playing field in smaller operations (IT Security Cluster). Second, some institutions provide lots of experience in designing learning pathways, reaching a significant number of learners and ultimately certify a qualification (Chambers of Commerce). Concerning the possibility to provide certifications, TÜV

Süd provides not only firm- and personnel certifications also specifically for SMEs, but they are also active internationally, e.g. in Italy with a sub-branch in Milano. Finally, with Bitkom a large multiplier exist that is very well known among all firms in Germany and that is primarily concerned with the internet-economy.

2.3.1 National Certification Systems

The Assessment and Recognition of Foreign Professional Qualifications Act ("Recognition Act") entered into force on 1st of April 2012 and introduced a standardized national procedure and criteria for the assessment of foreign professional qualifications (around 450) regulated under federal law (e.g. teachers, educators, social pedagogues, engineers or architects) (Dorothea Fohrbeck 2012). With this act, the federal government fulfilled its obligation to translate the European directive 2005/36/EC on the recognition of professional qualifications into German law (Directive 1005/36/EC of the European Parliament and the Council on the recognition of professional qualifications 2005). Concerning unregulated professions, including state-certified technician, state-certified biological-technical assistant, state-certified commercial manager as well as further vocational or technical school education and training qualifications, the *Länder (i.e. every state of the federal republic)* are responsible to provide recognition processes (around 18), following the principle of subsidiarity in the education sector. Consequently, every state has issued its own Assessment and Recognition of Foreign Professional Qualifications Act. University degrees that do not certify job-specific skills and cannot be clearly associated with a German reference occupation (degrees in economics, for example) are not regulated by the Recognition Act.

Currently, there are several initiatives ongoing in Germany which aim at facilitating recognition of non-formal and informal learning. The most important initiatives are:

a) ValiKom

The VALIKOM initiative (“Validierung von non-formal und informell erworbenen Kompetenzen” – “Validation of non-formally and informally acquired competences”) was a pilot program by the German Ministry of Education and Research (BMBF) the Association of German Chambers of Industry and Commerce (DIHK) as well as the German Confederation of Skilled Crafts (ZDH) in the period of 2015-2018 (Valikom 2021). Currently, the succession program “ValiKom-Transfer” is in the final phase of implementation and will terminate in October 2021. The general objectives of the ValiKom project are to develop a standardized process for recording, reviewing, assessing and certifying job-relevant competencies of people without vocational qualifications. With the finalisation of the two projects, validation and certification will be available for 32 occupations from industry, trade, crafts and agriculture. The target group of the initiatives are domestic and foreign learners and workers, which have acquired competences which are relevant for their occupation but are unable to proof them qua a qualification, diploma or degree. To be able to participate in the program, people have to be 25 years or older and possess relevant occupational experience. It is recommended that the

demonstrated experience exceeds the tie of the respective occupational training by a factor of 1.5.

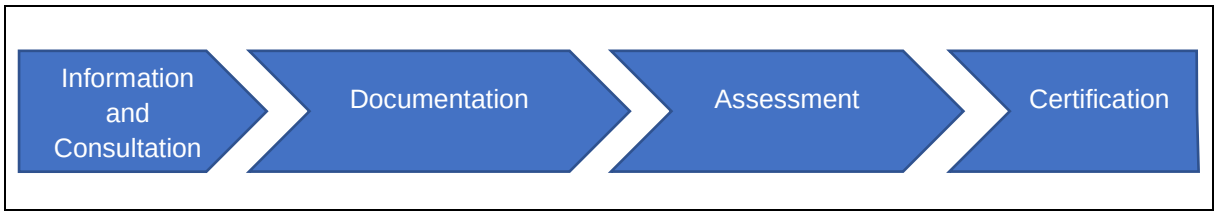

Figure 4: Certification Process for Non-Formal and Informal Learning

Source: Valikom (2018)

Certification process for non-formal and informal learning

Information and Consultation

Interested people can obtain initial information via the homepage of ValiKom and the websites of responsible authorities (especially the Association of German Chambers of Industry and Commerce). First of all, interested people should discuss with the contact person of the chamber in their area whether the process is suitable for them and whether they fulfil the admission requirements.

The contact person also assists in the selection of the reference profession. The reference profession corresponds to a recognized professional qualification. Besides, the contact person provides information about which documents are required for the process.

Documentation

The participants document their job-relevant experiences and competencies with a CV. After that they assess their professional competencies in relation to the reference occupation. Therefore, a self-assessment form is used. The assessment will be relevant for the decision, whether all or only individual fields of activity are evaluated in the external evaluation. The participants are supported by the responsible office, if they need help with the self-assessment.

Assessment

After the application has been submitted, the responsible authorities evaluate the documents submitted and passes them on to the evaluators. Evaluators are professional experts who carry out the external evaluation.

Before the external evaluation, a consultation takes place. In the meantime, the participants and the evaluators have the opportunity to talk about the requirements of the external evaluation and the fields of activity of the reference occupation. The self-assessment forms the basis for the discussion. The contents, instruments and procedure of the external assessment are also discussed.

The external evaluation is the most important part of the certification process for non-formal and informal learning. The participants get some practice-oriented tasks typical of the reference occupation so they can demonstrate their skills. While doing this, they are observed by the evaluators. Possible instruments with regard to the external evaluation could be work samples, case studies, presentations, role plays, etc. Finally, the evaluators assess whether the applicants are able to carry out the special field of activity and whether they have the necessary knowledge.

Certification

Depending on whether the applicants were able to perform all or only some of the fields of activity in the external assessment, they receive a validation certificate from the responsible authority. The validation certificate certifies the full or partial equivalence of the professional competences with the chosen professional qualification. If the competences of the applicants are not sufficient, the application will be rejected.

ValiKom represents a broadly developed and implemented initiative with the end to validate and certificate non-formal and informal learning. With 32 occupations already rolled out and the scaling of the project size among an increased number of participating chambers of commerce, it is expected that ValiKom will have a major impact on how validation processes will be conceived in Germany. It is important to note that ValiKom is capable to validate prior learning with the backdrop of existing occupational training curricula. Further, it validates only the entirety of the curricula, so that it is not capable of providing certifications for only parts of the entire competence set.

b) MYSKILLS

The Federal Employment Agency and the Bertelsmann Foundation have developed the test MYSKILLS. The project runs from November 2016 until November 2022. The test is especially intended for those people who cannot prove their informally or non-formally acquired competences so far. If you don't have a vocational qualification, it will be hard to find a job. Even if you have already worked successfully in a profession for several years and learned a lot there, you can hardly prove this in an application. The employer has difficulties assessing what the applicant is really able to do.
Especially the low-skilled workers are affected. Besides, it's a problem for immigrants and refugees. Work experience is usually not the problem - there is often a lack of appropriate certificates. MYSKILLS is designed to help certify informally acquired skills. Thus, it can help combat the lack of qualified personnel in many industries (Bertelsmann Stiftung 2021).

How does MYSKILLS work?

MYSKILLS is suitable for you if you have relevant experience in one of the 30 professions of MYSKILLS. The test is voluntary and free of charge and is available in several languages like English, German, Russian or Turkish. MYSKILLS is available for 30 jobs, e.g., for automotive mechatronics technician, horticulturist, cook, baker.
Before you start with the test, you can check out the website www.meine-berufserfahrung.de. There you can assess for yourself how much experience you have

already gained in a profession. In addition, you will get an impression of what other skills are required in this profession. Based on your self-assessment, you can decide in consultation with your advisor at the employment agency or job center for which job you would like to take the MYSKILLS test. Possibly several professions can be considered. The test takes 3-4 hours and consists of about 125 job-specific questions. The test can be taken in all employment agencies and job centers.

With regards to partial certification, the project “SEIZE THE OPPORTUNITY! With partial qualifications towards a vocational qualification” (DIHK 2021) has to be mentioned. The project “Seize the opportunity! With partial qualifications towards a vocational qualification” was established by the Federal Ministry of Education and Research and the German Chamber of Industry and Commerce in 2017. The aim is to create further qualification for low-skilled workers and give them a chance to acquire a vocational qualification. Many semi-skilled and unskilled workers have already acquired job-relevant skills, e.g., through employment or internships. However, most of them do not have suitable certificates that document this professional knowledge and skills in a comprehensible and comparable manner.

Together with the chambers of industry and commerce, the project “Seize the opportunity” should help creating standardized framework conditions for post-qualification. Besides, the transfer of the results and experiences should be ensured throughout Germany. The project contributes to giving more unskilled and semi-skilled young adults the opportunity to acquire a vocational qualification or at least further qualifications.

3 Austria

3.1 Background Information

Considering the Austrian education system in its entirety, a consideration at a glance provides some interesting insights. The illustration provided in Figure 5 is only exemplary to illustrate the many layers of the system. It is recommended to inspect the details via the corresponding website from OEAD. To the document is also referred to in **Appendix I** to this document, where the illustration is provided in detail and all levels are shown in German and English.

Please visit the official site on (OEAD 2021b) where you get very detailed information on all grades, age groups and educational levels via the interactive map of the screenshot below.

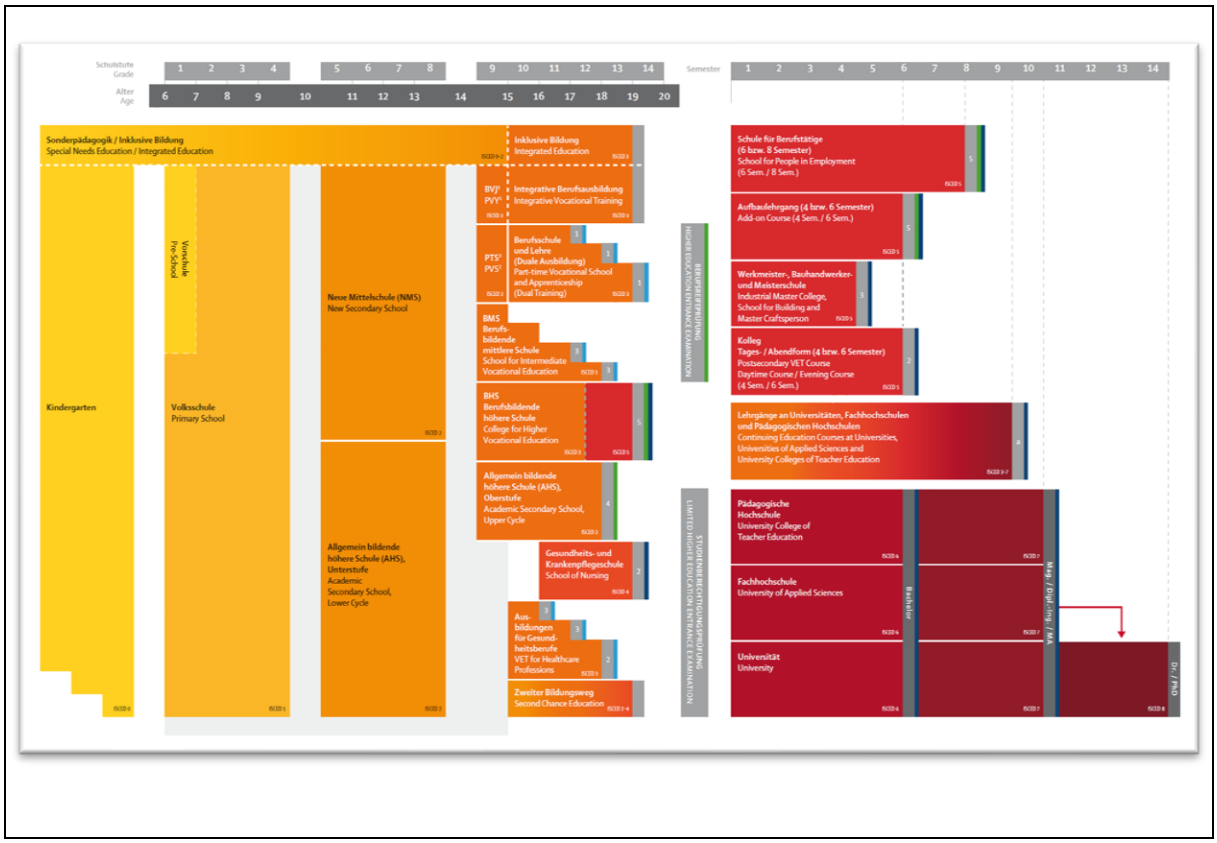

Figure 5: The Austrian Education System
Source: OEAD (2021b)

Please note, that the International Standard Classification of Education (ISCED levels) is included in the interactive map. ISCED helps educational researchers and educational policymakers compare, analyse and enhance the education systems in the OECD area with currently 34 member states. As ISCED levels have been specified from pre-primary education to university, they help experts and partners in other countries understand better and more quickly which educational level is achieved upon completion of a particular programme (OECD et al. 2015).

The "Second Chance Education" in Austria

The level of education that seems to be particularly interesting for our project is Secondary Level II, whereby special mention should be made here of the area of "Second Chance Education" (BMBWF 2020c).

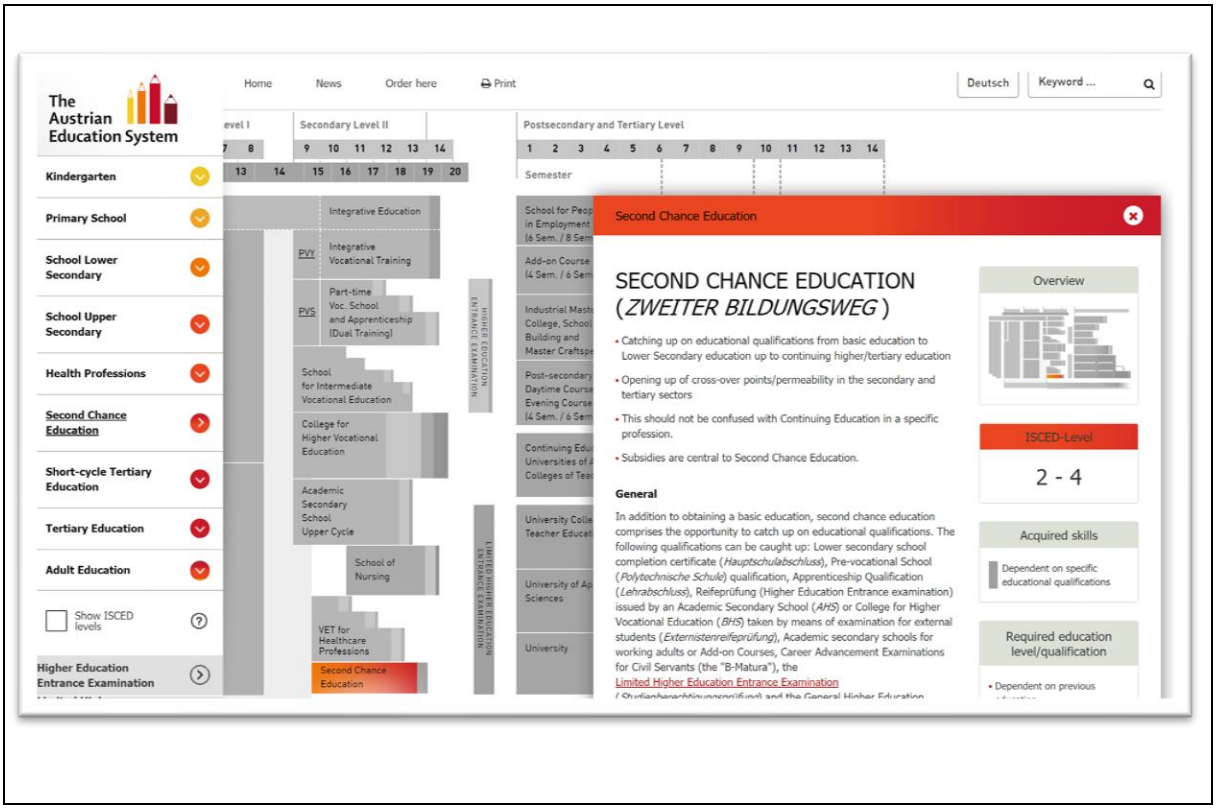

Figure 6: The second Chance Education in Austria
Source: OEAD (2021c)

Here is a summary of the most important facts for our project from the official website https://www.bildungssystem.at/en/second-chance-education:

- Catching up on educational qualifications from basic education to Lower Secondary education up to continuing higher/tertiary education
- Opening up of cross-over points/permeability in the secondary and tertiary sectors
- This should not be confused with Continuing Education in a specific profession.
- Subsidies are central to Second Chance Education.

In addition to obtaining a basic education, second chance education comprises the opportunity to catch up on educational qualifications. The following qualifications can be caught up: Lower secondary school completion certificate (Hauptschulabschluss), Pre-vocational School (Polytechnische Schule) qualification, Apprenticeship Qualification (Lehrabschluss), Reifeprüfung (Higher Education Entrance examination) issued by an Academic Secondary School (AHS) or College for Higher Vocational Education (BHS) taken by means of examination for external students

(Externistenreifeprüfung), Academic secondary schools for working adults or Add-on Courses, Career Advancement Examinations for Civil Servants (the "B-Matura"), the Limited Higher Education Entrance Examination (Studienberechtigungsprüfung) and the General Higher Education Entrance Examination for leavers of the apprenticeship training and VET schools (Link) (Berufsreifeprüfung). Though educational qualifications provide no guarantee of social security and professional advancement, they do however increase one's chances in the labour market, reduce the risk of unemployment and enhance the holder's personal development as well as access to further education. In the case of Second Chance Education, significant emphasis is placed on informing interested parties as to the types of subsidy that are available, as the participation in Continuing Education amongst adults is heavily dependent upon the financial resources and the amount of time available (BMBWF 2020a).

Catching up on qualifications taken upon completion of compulsory school education appropriate for adults (erwachsenengerechter Pflichtschulabschluss ePSA)

For students catching up on qualifications taken upon completion of compulsory school education appropriate for adults, examinations must be taken in six areas of competency. These examinations consist of four compulsory subjects (German, English, Mathematics and Careers Orientation) as well as two elective subjects (four elective subjects can be selected from: "Creativity and Design", "Health and Social Care", "Nature and Technology" plus an additional language). All examinations, with the exception of one, can take place at adult education institutions that have obtained authorisation to conduct examinations. A type of examination taken as an external student to obtain qualifications from a Middle School or a Lower Secondary School is also available. Preparation by following a course is not compulsory for all examinations taken as an external student and can even be carried out by means of independent study. If this is the case, the examination is taken at a school and not at an adult education institution. Catching up on qualifications taken on completion of compulsory school education enables those who successfully complete the programme to access School for Intermediate Vocational Education, Upper Level Academic Secondary Schools (AHS) and Upper Level College for Higher Vocational Education (BHS), Higher Technical College (HTL), Commercial College (HAK), etc.

Schools for Adults, Evening Academic Secondary Schools and Tertiary Continuing Education

Persons who have already entered the labour market or have completed a course of technical or vocational education, may obtain appropriate educational qualifications by attending courses that take place during the evening. Medium Level and Upper Level Secondary General, Technical and Vocational Schools for Adults, Add-on Courses (Aufbaulehrgänge), Post-secondary VET Courses and Academies are available. In Evening Academic Secondary Schools, i.e. state public schools, people under

employment are given the opportunity to take the Reifeprüfung (Higher Education Entrance Examination) in Second Chance Education. Preparation for this can either take place via courses offered by the schools or via distance learning. In addition, a range of Continuing Education is offered at universities, private universities, University Colleges for Teacher Training and Universities of Applied Sciences. University of Applied Sciences-Study programmes (Fachhochschul-Studiengänge) are also available for employees (BMBWF 2020b)

From Hafelekar's point of view, we can say that one big advantage of the Austrian education system is that there is a certain openness, i.e. "you always get a second chance" if you are interested in re-entering or continuing education within the formal education system.

The question that remains open is how continuing education outside this formal framework is valued. What happens to all the programmes, courses and training offered in the non-formal sector? In this respect, according to Hafelekar's analysis, the picture is not very encouraging. In the chapter 3.2.2 we address the issue of validation, which is still in its initial stages in Austria.

3.1.1 Legal Environment of Information Security in Austria

The fact that large areas of daily life are no longer functional today without the use of information technology systems is increasingly bringing the question of the security of information and data protection to the fore. Methodical security management is essential to ensure comprehensive and appropriate information security.

Information Security in Austria

The Austrian Information Security Act 2002 defines the legal basis for the implementation of Austria's obligations under international law for the secure use of classified information.

The most relevant standards for information security can be found within the ISO systems, in concrete terms compliance to ISO/IEC standards 27001 and 27002 (BKA 2021): ISO/IEC 27001 (Information Security Management Systems - Requirements) describes the requirements relevant to the establishment, implementation, control, audit, maintenance and improvement of an information security management system. The Information Security Handbook refers to this in chapters 2 and 3: they describe the basic process of establishing information security in an authority, organization or enterprise and provide concrete guidance on developing the comprehensive and continuous security process.

ISO/IEC 27002 (Guideline for Information Security Management) describes concrete recommendations for activities to achieve the objectives of the measures. Here, concrete and detailed individual measures are described with instructions for their correct implementation on an organizational, personnel, infrastructural and technical level.

Data Protection

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. In Austria, this Directive was implemented by the Data Protection Act 2000 (BMDW 2021), Federal Law Gazette I No. 165/1999. After 25 May 2018, the Basic Data Protection Regulation (DSGVO) and the revised Data Protection Act (DSG) will form the basis of data protection law (see (DSB 2019), Federal Law Gazette I No. 165/1999. After 25 May 2018, the Basic Data Protection Regulation (DSGVO) and the revised Data Protection Act (DSG) will form the basis of data protection law (see (DSB 2019).

Austria is a typical example for the international legal situation. No special rules on workplace privacy, only little evidence of jurisdiction and an only slowly rising awareness of the importance of the topic shape the field of Austrian employee data protection.

A recently concluded study by the Chamber of Labour found out, that only one out of four ICT systems that would need compulsory regulation by a works agreement, concluded between the workforce representative and the employer, is actually regulated. One reason is that ICT is difficult to understand for workplace representatives as well as employers. Due to the fast advance of ICT, it is difficult to make up leeway (Gutwirth et al. 2015).

3.1.2 Information Security Education and Training in Austria

In Austria, the following training paths are possible in the field of IT: "apprenticeship" (via the dual system), "BMS" (vocational middle school,) "BHS" (vocational secondary school, e.g. commercial academy or higher technical college; incl. college and advanced training course), "Fachhochschule" (University of applied sciences), "Universität" (university), "Universitätslehrgang" (university degree course) as well as further training offers at various adult education institutions or training institutes (Arbeitsmarktservice Österreich 2021).

The increasing digitalization of society creates new potential risks and dangers, because more and more fundamental business processes are based on IT and the IT infrastructure. This increases the need of companies and organizations for trained professionals who can act as a link between management and employees and implement appropriate organizational and operational measures to achieve and maintain information security (Arbeitsmarktservice Österreich 2021).

However, when it comes specifically to "information security", the focus in Austria is on university education. Here are the possibilities on University Level:

Title:	Certificate:	Duration:
Information Security	Master (FH)	4 Semester
Information Security Management (MSc)	University course	4 Semester
Business Informatics	Bachelor (FH)	7 Semester
Management & Digitalization	Bachelor (FH)	7 Semester
IT-Security	Bachelor (FH)	6 Semester

For **Data Protection it is different, because** the offer is more on “Data Management”, e.g.

Title:	Certificate:	Duration:
Data and Information Science	Master	4 Semester

Existing further training offers in Information Security are mostly related to ISO 27000 (See Appendix I).

Existing further training offers in Data Protection are also related to ISO 2700X are only short courses on GDPR (with no official certification) (See Appendix I).

3.1.3 Information Security Labour Market in Austria

Legal Guidelines on IT and Data Security in Austria

According to the Austrian Commercial Code (UGB) and the Limited Liability Companies Act (GmbHG), the responsibility for 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. 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).

With the NIS Directive (EU) 2016/1148, 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 WKO (Wirtschaftskammer Österreich), the Austrian Chamber of Commerce, offers 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 (Wirtschaftskammer Österreich 2020).

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 Chamber of Commerce's "IT Safe" is a well-established and well-known initiative to support SMEs in implementing IT security measures (Wirtschaftskammer Österreich 2021).

We discuss problems of SMEs in detail in chapter 3.

3.2 Institutional Landscape

For a concise overview see Appendix II to this document.

3.2.1 Stakeholder Analysis

There are plenty of stakeholders to be addresses concerning the fostering of information security for public interest, the improvement if information security education and the alteration of validation policies and practices. The Austrian government has sidelined the political will of rebuilding the Austrian economy on digital grounds with the institutionalization of competences across agencies and initiatives. Unfortunately, the there is still a clear focus on security missing, meanwhile education receives partially ressources. Concerning the provision of training, many providers have been identified which are predestined to carry out trainings across all EQF levels. Finally, institutions for the support of partial qualification have been identified. Meanwhile the implementation remains week, strong actors exist which support in the formal creation of programmes, which address content wise the needs of the project. Finally, authorities exist which are dedicated to the security of digital and private data.

However, it become apparent that stakeholders are not well connected among each other, and that a singular entity is missing that connects the need of educational institutions, public authorities and private companies. There are several IT expert associations, universities, business agencies and providers, that could dialogue with the local partner and connect the interests among each other. Generally, in the field of IT security and data protection (the two main project domains) Austria shown a great network, at national or regional / local level.

Further, “best practices” for the project have been identified: “KMU.Digital 2.0” is a funding program for SMEs in the field of digitalization processes. This promising initiative addresses as the main project target group small businesses; and, in general, the first obstacle for the implementation plans could be their level of awareness.

In general, the Austrian ecosystem is very well organize, including the NQF – National Qualification Framework point/body. NQF will play a key role, in Austria, for their “national implementation plan”.

3.2.2 National Certification Systems

In Austria, the areas of information security and data protection are strictly regulated by law.

The responsibility for IT security always lies with the management according to the Commercial Legal Code (UGB) and the GmbH Act (GmbHG). Even if security-relevant IT tasks are handed over to employees, the company management is ultimately responsible for compliance with the legal regulations. The EU Basic Data Protection Regulation (GDPR) and the Austrian Data Protection Act regulate the handling of personal data (e.g. name, date of birth, e-mail address, IP address).

With the NIS Directive (EU) 2016/1148, which was implemented in Austria at the end of 2018 by the Network and Information Systems Security Act (NISG), comprehensive regulations in the area of cyber security for strategically important companies, digital service providers and authorities at European and national level have been introduced for the first time. 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.

As described above in chapter 1), in Austria, training in the field of information security takes place in the university sector, which makes partial certification very complicated (impossible from the current point of view).

Validating and Transparency Tools in Austria

In Austria, there is no uniform legal framework to regulate validation and recognition of non-formal and informal learning. There is also no general individual right for individuals to access validation initiatives. The access requirements are defined for each initiative separately. The development of an explicit national strategy including all sectors on the validation of non-formal and informal learning commenced only recently.

National developments towards a national strategy for validation of non-formal and informal learning started in 2013 and are strongly linked to both the Austrian Lifelong Learning Strategy (UNESCO Institute for Lifelong Learning 2017) as well as to the development of the National Qualifications Framework (NQF). The Council Recommendation on validation as well as the implementation of the European Credit System in Vocational Education and Training (ECVET) also play an important role in this process. Steering groups and working groups have been set up for supporting coordination across sectors. Since the 2014 Inventory, important developments have taken place particularly in relation to the national validation strategy and the implementation of the NQF. Until now, there has been no uniform framework for validation and recognition of non-formal and informal learning in Austria (Bowden 2016).

In 2013, a working group (linked to action line 10 and measure 10.3 of the Lifelong Learning (UNESCO Institute for Lifelong Learning 2017) was established for the development of a national validation strategy. In 2015, a consultation document for the national validation strategy (including key objectives and measures) was published and there was also a national consultation process. The results of the consultation process were subsequently analysed and these were used to draft the national strategy for validation of non-formal and informal learning.

- The national validation strategy will also serve as the starting point for defining organisational structures and a detailed implementation plan for the coming years.
- The Austrian ECVET strategy was launched in 2014. One of its aims is to improve the recognition of competences gained in non-formal and informal learning contexts and thereby to support the implementation of the national validation strategy.
- The Austrian NQF entered the operational stage. In early 2016 a highly important milestone was achieved: a legal base for the NQF was adopted by the Austrian parliament and the NQF Act came into force in March 2016.

The high number of refugees that came to Austria in 2015 brought about an urgent need to understand their qualifications and competences in order to support their integration into the labour market as well as into society. To this end, the Austrian Public Employment Service (AMS) Vienna, for example, carried out a pilot project for people admitted as asylum seekers between August and December 2015, called ‘competence checks’ which included elements of validation of informally acquired competences. Further initiatives are currently being set up to address this urgent matter and a national validation strategy intends to provide them with a platform and framework for development and coordination.

The consultation document for the development of the Austrian validation strategy builds on the definition of ‘validation’ as presented in the Recommendation and suggests the following Country report: Austria 2 distinction (BMBF, 2015a): Based on their key objectives, two approaches for the validation of non-formal and informal learning are distinguished which could be closely interlinked and considered as steps or phases in a comprehensive validation process (BMB 2017):

- ‘Formative validation’ approaches are personal and individual-based measures which result in the proof of competences obtained independently of defined standards of the qualifications system. The focus is on the identification and documentation of competences.
- ‘Summative validation’ approaches are requirements - or standards - based measures which result in obtaining a qualification (or a part of it) of the formal or non-formal context, i.e. the competences of an individual are assessed and certified based on a relevant standard of a formal or non-formal qualification. The focus is on assessment and certification.

NQF - National Qualifications Framework

In Austria, the NQF Coordination Body (NKS) was set up to take over the central administration, coordination and information point for the NQF - i.e. the adaptation of the EQF - at national level.

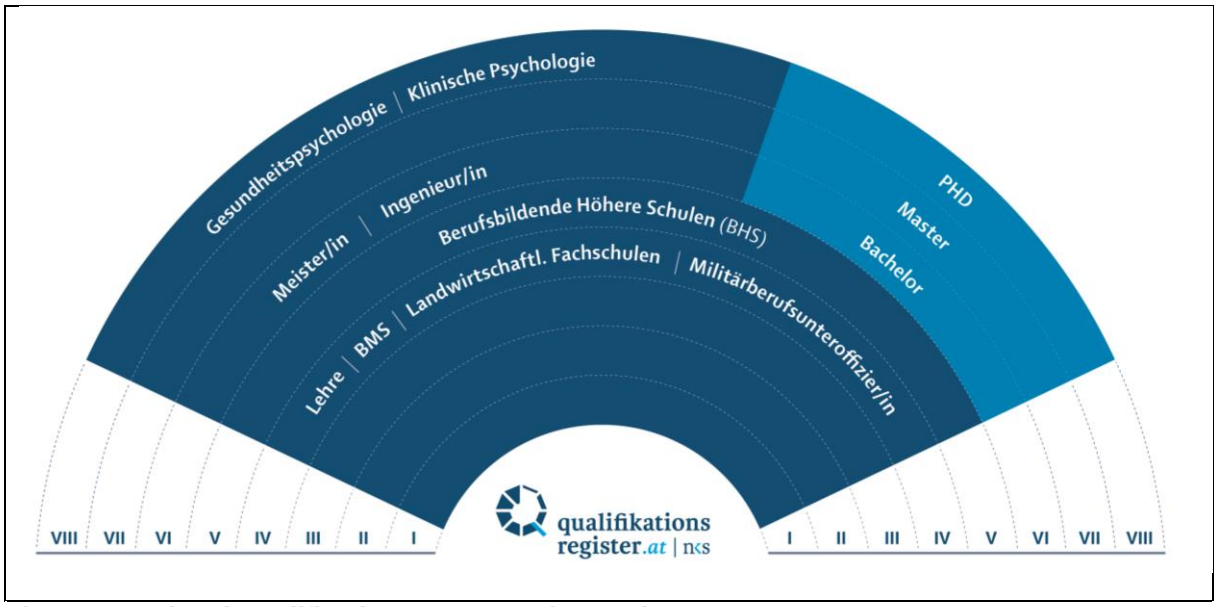

Figure 7: National Qualifications Framework Austria
Source: (OEAD 2021a)

The NQF is an instrument for classifying the qualifications of the Austrian education system. On the one hand, this transparency instrument should facilitate orientation in the Austrian education system and, on the other hand, contribute to the comparability and comprehensibility of national qualifications in Europe.

The aim is to make national qualifications and the Austrian education system understandable at European level, thereby promoting the cross-border mobility of learners and employees and supporting their participation in lifelong learning. Further aims are to increase the transparency of qualifications and to further develop learning outcomes orientation. The objective of the NQF Act (adopted in 2016) is to use the National Qualifications Framework as an instrument to promote the transparency and comparability of qualifications in Austria and Europe and to promote lifelong learning, which includes formal, non-formal and informal learning (OEAD 2021a).

Validation and NQF

In the further implementation of the NQF, both qualifications from formal education and qualifications acquired outside the formal qualification system (e.g. in continuing vocational training, adult education) should be able to be assigned to one of the eight levels. In the long term, it should be possible to acquire all qualifications reflected in the NQF, if possible, also by validation. The basic prerequisite for this is quality assurance based on learning outcomes and further development of methods and

procedures for validation. Learning outcome orientation is a central concept in the NQF and its implementation is a basic requirement for a functioning, recognised system of validation.

NQF service points

Since 15th of November 2019, the NQF service units have been operational and the NKS has started to allocate non-formal training and further training. NQF service points (NQF-S) are quality assurance sectoral bodies between providers of non-formal qualifications and the NQF Coordination Body (NKS). The reason for the establishment of such bodies is the diversity of non-formal qualifications on offer in adult education, further education and out-of-school child and youth work, and the high degree of freedom in the design of these offerings.

This poses particular challenges for the NQF classification of qualifications from this area, as there are no overarching responsibilities (regional, institutional, sectoral) or competencies for non-formal qualifications. NQF service points have two central tasks: On the one hand, they should assume an evaluation function in the assignment process with regard to the NQF compatibility of the respective qualification and the appropriateness of the assignment proposal, on the other hand they should support the qualification providers in the preparation of an assignment request and ensure the quality of the assignment request and the traceability of the requested NQF level. The NQF service centres are active on the initiative of qualification providers; in the non-formal sector, only they can submit a request for assignment, provided that the learning outcomes and their evidence are valid. A list of the six NQF service centres authorised by the BMBWF is available via (OEAD 2021a).

TeBelSi - The recognition process of TeBelSi Training as non-formal education in Austria

For the project we were in contact with the nationally responsible validation body, the "NKS - Nationale Koordinierungsstelle". In terms of content, the "NQF Service Point" at "ibw - Institut für Bildungsforschung der Wirtschaft" would be suitable for our project.

There are various forms of cooperation with the NQF service center at ibw. The type and scope of cooperation depends on the wishes of the qualification provider and the degree of NQF compatibility of the qualification. In principle, the NQF service center at ibw offers two service packages, a basic package with a lump sum of EUR 2,100 invoiced. Or the developer package with a lump sum of EUR 10,500 invoiced. Further services (e.g. supplements not covered by the two packages) will be charged separately on the basis of a daily rate of EUR 680 (Tritscher-Archan 2020).

The recognition of TeBeISi Training by professional associations

Individual professional associations and public institutions of youth welfare in Austria have an obligation to provide further training, which can be completed in courses at recognized training institutions. Further, it is possible to apply for recognition from individual associations or institutions.

The recognition of TeBeISi Training as formal education in Austria at University Level

If the TeBeISi Training is provided by an Austrian Full University or Applied University in the framework of existing Bachelor or Master Programme, it can be recognized (as part of the study programme) based on the ECTS System.

4 Lithuania

4.1 Background Information

4.1.1 Legal Environment of Information Security in Lithuania

In Lithuania situation with information security and data protection could be called legally stable, but practically fragmented. Despite the solid legal base and presence of controlling institutions, the threats for information security and personal data are increasing every year. As a member state of European Union (EU) Lithuania was obliged to incorporate General Data Protection Regulation (GDPR) on 25th of May, 2018. This document was a result of privacy and data protection reform in EU and was created to replace directive 95/46/EC. Despite the fact that legal norms were changed according to GDPR, the internal and external pressures are getting stronger forcing state institutions and business organizations to take the issue of information security and data protection more seriously.

Information security in Lithuania faces two main threat vectors. First one is related with the activity of cyber criminals and opportunists who target private and public internet infrastructure for malevolent purposes or just by testing the robustness of the security barriers. Second vector off threats comes from foreign adversaries that are trying to tamper ICT infrastructure or to affect processes within the country through public and private actors. The activities of cyber criminals and opportunists can be observed through various information security incidents that are being leaked to public media. In recent years there were significant information breach damage done to transportation, higher education, medical, and other business organizations. Cyber criminals usually demand ransom money for the stolen data or try to sell them online to the highest bidders. In some cases, private information is being released to public. There were instances when insufficient security in websites of physical infrastructure resulted in damages and data losses. At the same time, State Security Department of Lithuania announces the reports of “Annual threats evaluations” where significant portion of content is usually attributed to information security and data protection. In the recent reports it was noted that foreign actors actively try to tamper public and private information networks, websites, and services. It is noted, that with the years the complexity and aggressiveness of these attacks are getting higher.

The implementation of GDPR in EU member states is direct. However, EU leaves some freedom of discretion for the member states to specify certain parameters of legal data protection architecture. One of the most important laws in this area is the Amendment of Law on Legal Protection of Personal Data (No I-1374). This legal act specifies certain procedures defined in the GDPR. It also codes the basis of control institutions such as State Data Protection Inspectorate. There are also some changes related to GDPR in the Labor Code of the Republic of Lithuania. Finally, the Law on Cyber Security establishes cyber security principles and responsible institutions in the country.

The new and existing regulations increased the upkeep costs of the private and public organizations since new positions, like data protection officer, were introduced. The GDPR also forced to change interfaces of websites to better information about cookie policies, strengthened data gathering and saving requirements, affected other procedures, that involved the operations with personal data. From the business standpoint this burden was forced upon them without satisfactory support mechanisms. Smaller companies needed to find suitable people within to take data protection officer positions since hiring such professionals from outside would be costly. This was a serious challenge since competences required for such specialists are legal and ICT related. Despite the fact that information security and data protection requirements are increasing the costs of the business, intensified activities by cyber criminals and foreign adversaries raised awareness of the public and private organizations, and allowed realizing the seriousness of information security and data protection in current day and age. With that said there is still lack of support mechanisms that could allow private and public organizations to train or find the appropriate specialist more easily.

4.1.2 Information Security Education and Training in Lithuania

The system of education in Lithuania includes the following stages:

- **Pre-school and pre-primary education.** In Lithuania, early childhood education and care is composed of pre-school and pre-primary education and is attributed to the type of non-formal education.
- **Primary and lower secondary education.** Children must start attending primary schools when they turn 7 years of age during the calendar year. Education is compulsory until the age of 16. Primary and lower secondary education is free of charge in public educational institutions. Primary education lasts for 4 years. Lower secondary education lasts for 6 years and is also compulsory. It is delivered by pre-gymnasiums, lower secondary education schools, gymnasiums, school-multifunctional centres and vocational education and training (VET) schools. Education is compulsory until 16 years of age. By that time the learner will have usually finished the course of lower secondary education (10 grades).
- **Upper secondary and post-secondary non-tertiary level.** The two-year upper secondary curriculum is implemented by gymnasiums. VET schools along with a vocational education and training curriculum may provide the basis for the last two years of the lower secondary curriculum and/or upper secondary curriculum. Post-secondary non-tertiary curriculum is provided in VET schools and other institutions. Students typically aged from 17 to 19 learn there. A vocational education and training curriculum lasts from 1 to 2 years. Vocational education and training can be organized in school or apprenticeship formats.
- **Higher education.** Higher education comprises two types of institutions: universities and colleges. Learners can begin their higher education after gaining an upper secondary education. The degree structure follows a three-cycle structure: Bachelor's, Master's and Doctoral-level studies. The first cycle of studies

(Bachelor's) usually lasts for four academic years, the second cycle (Master's) two years and the third cycle (Doctoral) four years. Starting in 2018, short-cycle studies were introduced into the higher education system. Short-cycle studies are intended for the acquisition of the Lithuanian qualification framework's Level V qualification (ISCED 5). VET schools together with colleges can provide joint short-cycle studies after coordination with the Ministry of Education, Science and Sport.

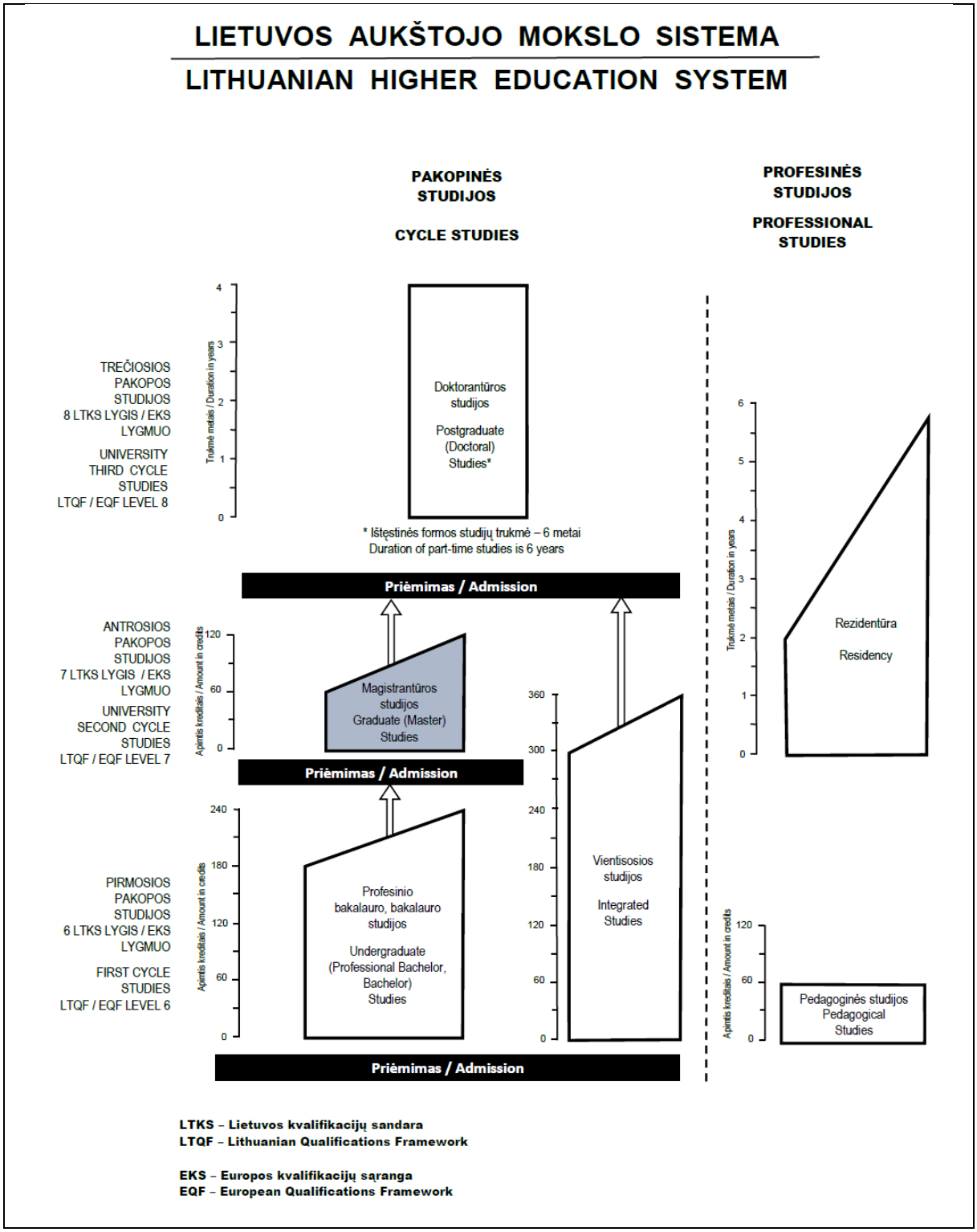

Figure 8: Lithuanian higher education system

The Centre for Quality Assessment in Higher Education (SKVC) is an independent public agency. The Centre implements the external quality assurance policy in higher education in Lithuania and contributes to the development of human resources by creation of enabling conditions for free movement. The main function of the Centre is to assist HEI to assure quality and to constantly improve it. The Centre fulfils this function through:

- Assessment of the quality of higher education;
- Assessment of the qualifications concerning higher education;
- Provision of information on higher education systems and qualifications recognition.

What formation/ education exists, which deal with information security?

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".

It should be noted that under the EU General Data Protection Regulation from 2018, May 25 a large number of companies and all public bodies are obliged to prepare data protection officers for practical activities. So, there are several days of training for this officer.

An overview of existing training offers in the field of information security and data Protection, as well as study programs can be found in Appendix II.

4.1.3 Information Security Labour Market in 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 country 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.

Expert interviews were conducted on information security and personal data protection issues in Lithuania. Research 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:

It is required to ensure the security of personal data. However, the given the implementation costs of information technology security (e.g.: encryption), are not cheap (licenses, applications), and such technologies are not yet used (E1).

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:

I think big business does understand the significance, and in small business the application of GDPR requirements is somewhat limited. State institutions are building up muscle, especially Data Protection Inspectorate, Cyber Security Center <....> The database of the Personal Data Protection Inspectorate even contains an overview of practices on personal data protection violations in Lithuania and practices (E2).

Public attention to information security is also increasing by following public security incidents:

When a business hears about such a scandal [CityBee data leak], it then starts to pay attention, if we have the data protected. From practice, I can say that small businesses with little IT exposure do not provide IT services, so that data protection was more important only when the BDAR came into force. (E2).

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.

Often it depends on my own initiative. I find trainings that are relevant to me, present them to managers and usually they don't mind paying. For help with information security issues, please contact the company's data protection specialist, who gives the advice (E3).

Does not pay much attention to internal training. In Lithuania, there is an institution that provides consultations in the field of data protection, SMEs can apply for advice. However, is the SME being not always competent enough to understand when and on what basis to take consultations from the authorities (E1).

Now, in the case of Covid, it's really, no one does that training, everyone is trying to survive because it's a very difficult situation and that's why I think there's really no such training in small businesses. Because there are simply no funds for that ... Now we need to survive, and we will protect personal data later" (E2).

4.2 Institutional Landscape

See Annex II to this document for a concise overview.

4.2.1 Stakeholder Analysis

Meanhwile VET programmes are decentrally organized via vocational schools, alongside colleges mixed educational programmes (short cycle trainings) can be offered. These programmes are being coordinated by the central ministry of education. Specific actors have been identified which are capable to stir the interest of SMEs and Information security providers. Further, social partners exist which have an interest in piloting courses on a municipal level and support the implementation process of the TeBeISi project. Finally, stakheolders are active in the provision and strengthening of human rights in terms of information security and data protection in civic contexts.

In general, the field of actors is less diverse then in western European countries, and more spific stakeholders exist with an interest to engage in the TeBeISi project activities. Support can be expected with regard to piloting courses, offering certifications or working on project contents form these partners.

4.2.2 National Certification Systems

Lithuanian education policy documents identify the evaluation and recognition of non-formal and informal learning as one of the priority goals of the education system, emphasize the importance of universities' openness and flexibility in expanding the university study sector and building bridges between formal, non-formal and informal education; development by creating opportunities for adults at Lithuanian universities to seek recognition of learning achievements acquired in various learning environments. Evaluation and recognition of non-formal and informal learning in educational institutions (universities, colleges) and is evidence of their openness and flexibility, as it is recognized that not only learning in an academic environment is a value, but also in higher education. not only knowledge is created, but bridges are built between the world of work and academia.

In Lithuania, successful assessment of adults' non-formal and informal learning can result in their enrolment to an institution of HE and/or credit award (Republic of Lithuania 2015). Recommendations for higher education institutions on assessment and recognition of competences acquired through the system of adult non-formal education, In Lithuania, a number of HEIs started assessing adults' non-formal and informal learning in 2013 through the EU-funded projects; therefore, their primary task was to train the staff, including administrators, assessors and consultants so that to ensure the implementation of the process. It is obvious that to provide effective support and guidance to adults, it is essential to train competent consultants; thus, there exists a need to investigate novice consultants' experience and establish the challenges they face so that to deeper understand how to support the process.

Regarding the possibility to recognize (confirm) informally acquired competencies in the field of information security in Lithuania, the opinions of the conducted research experts differed: according to one expert, certifying informally acquired competencies would be useful only for data protection specialists as an entry in the CV. People working in the field of information security and personal data protection need knowledge, not a certificate. According to other experts, it is necessary to certify competencies in order to ensure the competence of these persons in the field of personal data protection. However, this would be relevant for businesses providing data protection services. However, according to the expert, the price of such services would rise immediately, and it would be difficult for professionals working in the public sector due to lack of knowledge. Perhaps certification would encourage businesses to learn more about personal data protection, and according to the expert, businesses may be reluctant to face administrative burdens during this difficult period.

It is a very sensitive situation and businesses will not want that administrative burden. But the idea would be similar to having someone responsible for work safety. So following the same example someone in a business should be responsible for protecting personal data. Sometimes it seems to me that the consequences of personal data breaches may be greater than work safety (E2).

5 Poland

5.1 Background Information

5.1.1 Legal Environment of Information Security in Poland

The information security is developed in accordance with the applicable legislation and based on the requirements of the Polish Standards in the area of information security, including in particular:

1) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of physical persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Official Journal of the EU L 119 of 04.05.2016, p. 1), hereinafter referred to as "RODO";

2) the Act of 10 May 2018 on personal data protection (Journal of Laws of 2018, item 1000 and 1669);

As of 25 May 2018, due to the entry into application of new regulations governing the issues of personal data protection and the entry into force of the new Personal Data Protection Act, the previously applicable requirements for documentation of personal data processing have ceased to be valid. Currently, all requirements in the above respect should be in line with the requirements specified in:

- Regulation of the European Parliament and of the Council (EU) of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC called the General Data Protection Regulation (GDPR);
- The Act of 10 May 2018 on the protection of personal data (Journal of Laws 2018, item 1000);
- Other national as well as European Union domain regulations, such as:

Regulation of the Minister of Health of 9 November 2015 on types, scope and models of medical records and the way they are processed,

- Regulation of the Minister of Science and Higher Education of 16 September 2016 on the documentation of the course of studies,
- Regulation of the Minister of National Education on the manner in which public kindergartens, schools and institutions keep records of the course of teaching, educational and caring activities and the types of such records,
- Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use and repealing Directive 2001/20/EC, and other.

5.1.2 Information Security Education and Training in Poland

At the level of secondary vocational education in Poland, only the ICT Technician profile is available, whose range of competences only to a small extent relates to the DP/IS professional profile, so it can be assumed that there is no such offer at this level of education. HE offer of studies at both Bachelor's (engineer) and Master's level is wide.

Examples of the offer:

- Andrzej Frycz Modrzewski Kraków Academy of Technology

field of study: computer science and econometrics - 3.5 years, engineering, practical character

Graduates of computer science and econometrics are able to develop and implement IT systems, create computer graphics and manage websites. They are also familiar with issues related to information security. Thanks to the skills acquired during their studies, they can find employment in industrial, commercial and service companies, banks, insurance companies, tax offices or public institutions.

- WSB Academy in Dąbrowa Górnicza, field of study: Information Security and Personal Data Protection, II degree, Master's degree

The aim of the specialization is to prepare graduates to perform the function of a Personal Data Protection Inspector (formerly ABI), fulfilling the knowledge requirements specified in the Personal Data Protection Act. The specialization prepares to work as a specialist in the field of information security, with particular emphasis on the challenges arising from the dynamic development of information technologies and in the field of managing and auditing the information security process in an organization.

- Wyższa Szkoła Bankowa, field of study: Information security and cyberspace, bachelor's degree

Graduates acquire knowledge of developing and implementing procedures related to information and information systems security, are able to select compatible systems and configure security systems, know how to manage local and network systems, understand the operation of electronic signature, know elements of cryptography and network traffic monitoring.

- Collegium Civitas, course: Inspector of Data Protection, post-graduate studies

Graduates know how to integrate personal data protection with the Information Security Management System (ISMS), learn the next steps related to personal data protection at the stage of designing IT systems, risk management methodology in personal data protection, and data protection impact assessment.

During practical classes they learn about the solutions for designing and implementing an Information Security Management System in an organization, necessary to achieve the assumed business goals, conduct a complete information risk analysis, and consequently also a data protection impact assessment (DPIA).

In Poland there is practically no education at EQF level 5 with the exception of exceptional solutions like teacher training colleges or social colleges. It also does not exist in the area of IS/DP.

Selected thematic course offerings

- short 1 or 2-day courses on narrow topics from as little as EUR 100

RODO ONLINE TRAINING Compact training discussing key issues in the field of personal data protection and principles of data processing based on the current legal regulations.

RISK ANALYSIS AND DPIA Training with workshop elements addressed to persons in charge of risk assessment and data protection impact assessment in the organisation.

- courses with EITCI certificate cost approximately 1000 EUR

5.1.3 Information Security Labour Market in Poland

It is very difficult and expensive to employ an expert who covers such broad areas of knowledge as law and IT and who additionally has the necessary social skills, which is why most SME's do not have such a person in their ranks.

Small and family businesses and one-man companies most often use external solutions, i.e. once in a while they consult an expert, e.g. a law firm, which helps them to adapt their solutions to the current law.

When we consulted the local BNI group in which small entrepreneurs are affiliated, we learned that among small businesses the greatest interest occurs when the law changes. In May 2018, when the new European directive came into force, numerous training sessions were organised and there was widespread awareness of the need to adapt to the new legislation. Later, after the relevant changes were introduced, interest in this topic definitely declined.

There is now somewhat more interest again due to the fact that a pandemic has broken out. Many companies had to move their operations overnight to the Internet and the conditions for them have changed again.

5.2 Institutional Landscape

See Appendix II of this document for a concise overview.

5.2.1 Stakeholder Analysis

Several institutions regarding the projects interest have been identified. Next to private companies, ICT experts and Training Academies, IT security points can be mentioned among stakeholders with an active intent to support the project. Meanhwile most of the stakeholders are private, the regional chamber of industry and commerce plays a crucial part concerning VET and certifications. Further, public organisations have been identified which stir the interest of regional companies, to provide a forum for experience and services exchange as well as to provide arenas for politicians and firms owners for the discussion of regional needs. Further dedicated training providers also for information security and data protection exist. Generally, Poland disposes of a rich and active internet economy and is prepared to tackle all sorts of challenges coming with increased digitalization. Therefore, an active market of service providers can be encountered. Finally, specific tasks concerning the project have been externalized from the government into specific institutions, which can be involved in the project implementation.

Due to the structure of the stakeholders, a strong involvement of SMEs can be expected. Finally, a stronger involvement action is needed, above all for the implementation phases (when the – part – certification framework should be presentated and shared with local / regional stakeholderds too).

5.2.2 National Certification Systems

In 2012 the standard “PN-ISO/IEC 27000 Information technology - Security techniques - Information security management systems - Overview and terminology” was published. The standard - a translation without any changes of the International Standard (“ISO/IEC 27000:2009 Information technology - Security techniques - Information security management systems - Overview and vocabulary”)- is one of the important documents organizing, clarifying, advising and introducing the Information Security Management System (ISMS) belonging to a number of standards listed below:

- PN-ISO/IEC 27001:2007, Information technology - Security techniques - Information security management systems - Requirements
- ISO/IEC 27002:2007, Code of practice for information security management
- ISO/IEC 27003:2010, Information security management system implementation guidance
- ISO/IEC 27004:2009, Information security management - Measurement

- PN-ISO/IEC 27005:2010, Information technology - Security techniques - Security risk management
- ISO/IEC 27006:2009, Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007:2011, Guidelines for information security management systems auditing
- ISO/IEC 27011:2008, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO 27799:2008, Health informatics - Information security management in health using ISO/IEC 27002.
- The PN-ISO/IEC 27000 standard can be used in all types of organisations, e.g. commercial enterprises, government agencies, charitable institutions.

Concerning validation systems of competences, Intensive work has been underway in Poland for several years to introduce changes in these areas. This involves not only the development of a system for validation, certification and transfer of learning outcomes and, consequently, of qualifications, but also the revision and standardisation of terminology. An overview of the Polish ualification Framework can be found enclosed:

Qualification levels	Certificates and diplomas confirming a given level of qualifications
Level I	Primary school leaving certificate: awarded to pupils finishing the 6-year primary school which was in place before the ongoing reform of the school education system 1st grade music school leaving certificate 1st grade general music school leaving certificate
Level II	Primary school leaving certificate: awarded to pupils finishing the 8-year primary school which has been established by the ongoing school education reform Lower secondary school leaving certificate: awarded to pupils finishing the lower secondary school which was in place before the ongoing school education reform
Level III	Diploma conferring vocational qualifications: awarded upon finishing a stage I sectoral vocational school, or achieving the same level of education through other equivalent education paths, and upon passing exams leading to qualifications for a given occupation Diploma conferring vocational qualifications: awarded upon finishing a basic vocational school, or achieving the same level of

	education through other equivalent education paths, and upon passing exams leading to qualifications for a given occupation Journeyman certificate: awarded upon finishing a basic vocational school or stage I sectoral vocational school and passing examinations for so-called craftsman occupations. The qualifications acquired should correspond to the level of qualifications identified in the PQF.
Level IV	Diploma conferring vocational qualifications: awarded upon finishing a technical upper secondary school or post-secondary school, or achieving the same level of education through other equivalent education paths, and upon passing exams leading to qualifications for a given occupation Art school diploma conferring a vocational title. The qualifications acquired should correspond to the level of qualifications identified in the PQF. Maturity certificate
Level V	Diploma of a teacher training college Diploma of a foreign language teacher training college Diploma of a college of social work
Level VI	First-cycle diploma
Level VII	Second-cycle diploma Long-cycle diploma
Level VIII	Doctoral / PhD diploma

Table 2: The Polish Qualification Framework

Source: Based on ustawa o Zintegrowanym Systemie Kwalifikacji z dnia 22 grudnia 2015 r. (Act of 22 December 2015 on the Integrated Qualifications System)

Extramural or external exams (which adults take as externals) are one of the methods of validating LOs achieved outside the formal education system. They enable validation of LOs achieved by adults choosing to prepare independently for exams at the level of primary or post-primary school which cover the requirements laid down in the national core curriculum for general education. In the case of schools providing vocational education, adults may also prepare independently for an exam leading to qualifications for a given occupation (extramural / external vocational exam). It is worth noting that an extramural / external vocational exam is not conducted for all occupations for which students are trained in the school education system; for example, it does not cover medical occupations (EURYDICE 2020).

In this context, it is important to highlight the Polish Integrated Qualification System (see (Zintegrowany System Kwalifikacji 2020), which was initially populated with full and partial qualifications from the formal education system. Progressively, more and more market qualifications are making an entrance into this system, providing for an innovative and flexible element in the education system across all EQF levels.

6 Italy

6.1 Background Information

The Italian education and training system is organized according to the principles of subsidiarity and autonomy of educational institutions. The State has exclusive legislative competence for the "general rules on education" and for the determination of the essential levels of services that must be guaranteed throughout the national territory. The State also defines the fundamental principles that the Regions must respect in the exercise of their specific competencies. The Regions have concurrent legislative power in matters of education and exclusive power in matters of education and professional training. State scholastic institutions have didactic, organizational and research, experimentation and development autonomy.

The educational system is organized as follows:

1) Integrated system zero-six years, non-compulsory, with a total duration of 6 years, divided into
   - educational services for infancy¸ managed by the local authorities, directly or through the stipulation of conventions, by other public bodies or private individuals, that welcome children between three and thirty-six months of age;
   - infant school, which can be managed by the State, by local authorities, directly or through the stipulation of conventions, by other public bodies or by private individuals, which welcomes children between three and six years of age;
2) first cycle of education, compulsory, with a total duration of 8 years, divided into
   - Primary school¸ lasting five years, for pupils from 6 to 11 years;
   - Secondary school, lasting three years, for students aged 11 to 14 years;
   - Second cycle of education articulated in two types of paths:
   - Secondary school, lasting five years, for students who have successfully completed the first cycle of education. Schools organize high school, technical and vocational institutes for students from 14 to 19 years of age;
   - Three- and four-year courses of vocational education and training (IeFP) of regional competence, also aimed at students who have successfully completed the first cycle of education.

Higher education offered by universities, institutions of Higher Education in Art, Music and Dance (AFAM) and Higher Technical Institutes (ITS) with different types of courses:

- tertiary education paths offered by universities
- tertiary education courses offered by AFAM institutions (High Artistic, Musical and Coreutic Education)
- professionalizing tertiary training courses offered by ITS (Istituti Tecnici Superiori).

Compulsory education

Compulsory education has a duration of 10 years, from 6 to 16 years of age, and includes the eight years of the first cycle of education and the first two years of the second cycle (Law 296 of 2006), which can be attended in the secondary school - state - or in regional vocational education and training paths.

In addition, the right/duty to education and training applies to all young people for at least 12 years or, in any case, until the attainment of a three-year professional qualification by the age of 18, in accordance with the provisions of Law 53/2003.

Compulsory education can be carried out in state schools and in parochial schools (Law 62 of 2000), which constitute the public education system, but it can also be carried out in non-parochial schools (Law 27 of 2006) or through family education. In the latter two cases, however, the fulfillment of the educational obligation must be subject to a series of conditions, such as the performance of qualifying exams.

The parents of the pupils, or whoever exercises parental responsibility, are responsible for the fulfillment of the obligation to educate minors, while supervision of the fulfillment of the obligation is the responsibility of the municipalities of residence and the school directors of the schools in which the pupils are enrolled. At the end of the period of compulsory education, usually scheduled at the end of the second year of secondary school, if the student does not continue his studies, a certificate of the skills acquired is issued (Della Istruzione 2007)**.** After passing the State examination at the end of secondary school, the student can access tertiary education courses (university, Afam and ITS). Some university courses have a limited number of students and students must pass an entrance test.

Non-state education

Article 33 of the Italian Constitution establishes two fundamental principles: the State's obligation to offer a state school system to all young people and the right of physical and legal persons to create schools and educational institutions without charge to the State.

A Qualifications Framework (QF) is a valid tool for the description of all or part of the qualifications referring to a national system or, more generally, to various systems between themselves, as well as being a useful tool to understand the whole set-up of an education system. The descriptive methodology used in a QF is based on the classification of the qualifications in different levels, which are differentiated one from another according to other descriptors called learning outcomes, which describe the results – in terms of capability, knowledge and ability – which the holders of the

qualifications positioned at a given level will have acquired with the issuance of an academic qualification or of a professional certification. In all cases of foreign qualification evaluation, the existence of a national qualifications framework is certainly supportive and of help with regard to the understanding of the education system referred to.

In 2005, the Ministers of Higher Education of the Bologna Process signatory countries decided to develop the Qualifications Framework for the European Higher Education Area - QF for the EHEA. The Framework comprises the three main cycles of Higher Education, as defined by the Bologna Process, and offers an overview of all qualifications awarded at the end of each cycle, with reference to the number of ECTS credits collected and to the learning outcomes according to the Dublin Descriptors. The Qualifications Framework for the European Higher Education Area is aimed at facilitating the correct understanding and comparability of qualifications in the higher education systems of each country. A further aim of the framework is to offer a comprehensive overview of the European teaching and learning offer, targeted at students coming from all over the world. Each country committed to putting together a National Qualifications Framework – NQF which is compatible with the Qualifications Framework for the European Higher Education Area.

In 2005, the Italian Ministry of Education, University and Research (MIUR) started working on the Italian Qualifications Framework, in compliance with the procedures established at European level. CIMEA was tasked with producing the first prototype model of the National Framework and, after a process of national consultation, the Italian Qualifications Framework – QTI was published in 2010.

6.1.1 Legal Environment of Information Security in Italy

The fact that large areas of daily life are no longer functional today without the use of information technology systems is increasingly bringing the question of the security of information and data protection to the fore. Methodical security management is essential to ensure comprehensive and appropriate information security.

Information Security in Italy

The most relevant standards for information security can be found within the ISO systems, in concrete terms compliance to ISO/IEC standards 27001 and 27002 (BKA 2021).

ISO/IEC 27001 (Information Security Management Systems - Requirements) describes the requirements relevant to the establishment, implementation, control, audit, maintenance and improvement of an information security management system. The Information Security Handbook refers to this in chapters 2 and 3: they describe the basic process of establishing information security in an authority, organization or enterprise and provide concrete guidance on developing the comprehensive and continuous security process.

ISO/IEC 27002 (Guideline for Information Security Management) describes concrete recommendations for activities to achieve the objectives of the measures. Here, concrete and detailed individual measures are described with instructions for their correct implementation on an organizational, personnel, infrastructural and technical level.

Data Protection

In the year of the health emergency, the market held up: 40% of large companies increased their cyber security budget (51% in 2019), 19% reduced it (2% the year before), 52% of spending dedicated to security solutions, 48% to services. Network & Wireless Security, Endpoint Security and Data Security are the types of security attracting the most resources

Cyber security management is still not very mature: only 41% have a CISO. The Data Protection Officer is present in 69% of the organizations, the rest rely on external figures

Research by "Observatory Cyber Security".

2020 was also a year of emergency on the cyber security front. For 40% of large companies, cyber-attacks have increased compared to the previous year. The sudden and widespread spread of remote working and agile working, the use of personal devices and home networks, and the boom in collaboration platforms have in fact increased the attack options available to attackers.

The economic impact of the pandemic has forced Italian businesses to meet increased security challenges with reduced budgets: 19% have decreased their cyber security investments (down from 2% in 2019) and only 40% have increased them (it was 51% the year before). But for more than one in two companies (54%), the emergency was a positive opportunity to invest in technology and increase employee awareness of security and data protection. Overall, the Covid-related crisis19 slowed the growth of the cyber security market but did not stop it.

In 2020, spending on cyber security solutions reached €1.37 billion, up 4% from the previous year (in 2019, the market had marked an 11% increase over 2018), 52% of which is accounted for by security solutions and 48% by services. Investments in cyber security are mainly related to emergency management, as evidenced by the growth in Endpoint Security spending. Cloud, Smart Working and Big Data are the digital trends that have most influenced security management in the last twelve months. Also noteworthy are Operational Technology (OT) Security, which sees an acceleration in investments, and Artificial Intelligence, used in cyber security by 47% of companies.

Despite a growing market and the increasingly strategic role of cyber security, companies still have little organizational maturity. Only 41% of companies have a CISO responsible for cyber security, and 38% of companies have no communication with the

Board on this topic. The management of data protection is more evolved, also due to the regulatory push, with 69% of companies that have included a Data Protection Officer (DPO) in the workforce and the rest using external figures.

These are the results of research by the Cyber security & Data Protection Observatory of the School of Management of the Politecnico di Milano, presented today during the online conference "Cyber security Odyssey: the key to evolve".

2020 has been a real odyssey, with an unprecedented increase in cyber attacks, the need to reorganize to manage the sudden boom in smart working and the rationalization of the budget available to meet security challenges due to the serious economic impact of the pandemic.

Despite the negative context, the market has not stopped growing and most companies have taken the opportunity to invest, renew themselves and increase the sensitivity of employees on the issue. Cyber security can be the key to evolve and manage the changes taking place, but it must be managed in a more mature and strategic way.

The Italian cyber security market, however, is still limited in relation to GDP, with an incidence of just 0.07% in 2019, about 4-5 times less than the most advanced countries. And the research also shows the need to strengthen regulatory oversight, also considering the penalties imposed by the competent authorities and the important data breaches that have been reported during the year.

Anatomy of the Cyber security market

The type of security that attracts the most investment is Network & Wireless Security (33%), the strategies and solutions that protect infrastructure from damage and improper access. This is followed by Endpoint Security (23%), which is the protection of each device connected to the network, and Data Security (14%), the systems to protect company and individual user data. Cloud environment security is worth 13% of spending, Application Security 12%, while IoT security is still marginal (3%). Finally, there is another residual category that occupies the remaining 2%, which mainly includes cyber security awareness and training initiatives.

Spending is split almost 50/50 between security solutions, with 52% of the market, and professional and managed services, with 48%.

The solutions that companies invest most in are systems to monitor security events (16%), manage and monitor user access to data and applications (14%), assess the vulnerability and security of systems, applications or networks (14%), analyze the cyber risk exposure of enterprise systems and assess their compliance with security standards (12%) and solutions that monitor network traffic to identify and block unauthorized access (11%).

Among services, 51% of spending is on Professional Services, services offered by vendors outside the company for a specific project, while 49% is on Managed Services,

services offered on an ongoing basis by external vendors to maintain company information systems.

Trends in Cyber security and Data Protection

The Cloud is the trend that has most influenced cyber security management in companies, together with Smart Working and Big Data. In the last year, edge type Cloud services have emerged, extending the boundaries of the cloud, but companies still complain about a lack of threat awareness on the part of top management (74%), an increase in attacks that is more evident than in other areas (64%) and difficulties in relating to cloud service providers because they have little negotiating power (74%) or struggle to carry out security assessments (66%).

Among the other most relevant trends, the acceleration of investments in OT security, which, however, is not accompanied by an adequate maturity: only one company out of two has introduced OT security policies and less than a third provides specific training on the subject.

Artificial Intelligence remains a topic of interest for companies, which use it in the field of cyber security in 47% of cases (but only in 14% in a significant way), especially to identify new threats (68%) and to monitor the behavior of systems and users in order to detect anomalies (66%).

The importance of Supply Chain Security, the protection of third-party systems and networks, is also growing, but so far only 13% of the sample has put in place technical tools and formal organizational control.

Security and Data Protection skills

The management of cyber security and data protection requires specific profiles and skills.

As far as the area of IT security is concerned, the situation has not recorded any evident changes in the last year: only in 41% of companies the responsibility is entrusted to a formalized CISO, in 25% it is in the hands of the CIO, in 13% to a CSO or security manager, while in the remaining cases it is in the hands of another company figure (19%) or there is no dedicated figure (2%).

In 38% of the organizations analyzed, there is no periodic report to the Board of Directors by the figure responsible for security on the actions taken.

Data protection is managed in a more advanced way, with the DPO present in the staff of 69% of companies and as an external figure in the rest of the sample. In 51% of cases, this figure reports directly to the board and in 52% has a dedicated budget (+9% on 2019).

Italian SMEs and Cyber Security

Smaller companies have struggled to adapt to the new models of work organization imposed by the emergency. According to 59% of SMEs surveyed by the Observatory, the use of personal devices and home networks has exposed companies to greater security risks, and for 49%, cyber attacks have increased.

Although cyber security is starting to become a priority, SMEs are still struggling to translate perceptions into reality: only 22% have planned security investments for 2021, 20% had planned them but had to reduce their budgets following the emergency, a third have no budget to devote (32%) and over a quarter are not interested in the subject.

Those who do invest focus primarily on the technological component: 41% intend to invest in basic security solutions, such as antivirus or firewalls, while 37% are looking at more sophisticated solutions, such as Intrusion Detection or Identity & Access Management systems.

As for cyber security management, 32% of the sample has invested in security and data protection training for employees, 28% have turned to consultants to improve cyber security management in the company, 18% have introduced dedicated skills such as Security Analyst or Security Administrator, and 15% have taken out insurance policies to transfer cyber risk.

The regulatory framework and the challenge of compliance

The European data protection and cyber security regulatory framework has evolved in recent years, with the GDPR, the NIS Directive and the Cyber security Act in particular coming into force. At the end of 2020, the European Commission published a new package of measures to implement a strategic plan on cyber security for the next five years, increase the resilience of networks and infrastructures and fight cybercrime. In Italy, the "National Cyber Security Perimeter" has been adopted.

However, there are still many challenges to be faced by companies and institutions, starting with strengthening compliance. Another "crucial" challenge is the difficult relationship between technological innovation and data protection.

In an era of digitization and technological progress, it is necessary to wisely balance the opportunities offered by new technologies with the protection tools made available by the regulatory framework on data protection: digital transformation and technological innovation, in the absence of adequate intervention measures, would produce negative effects without bringing any benefit.

6.1.2 Information Security Education and Training in Italy

Overview of jobs offered in the field of Information Security and Data Protection

One of the aspects highlighted by the experts, particularly in the last two years, is the need for the right skills. Companies are therefore gearing up to strengthen their security management teams. Four out of ten large companies (39%) expect an increase in the number of roles that manage cybersecurity and almost half (49%) say that it will increase the number of figures responsible for managing privacy.

The new professions in the security field what are the emerging figures?

Certainly the Chief Information Security Officer (CISO), for whom the responsibilities and competences required increase. In addition, other figures with specialist roles emerge, such as the Security Administrator, a figure already foreseen, included or in any case screened in 76% of the sample analysed: it deals with making the technological security solutions operative; other figures of growing interest (for 57% of the sample companies) are the Security Architect, to whom the verification of the security solutions present in the company is delegated, and the Security Engineer (56%), who monitors the systems and suggests ways of responding to the incidents.

A close distance from business desires is the Security Analyst (55%), which analyzes potential vulnerabilities of systems, networks and business applications. Another interesting figure is the Ethical Hacker (39%): he identifies who has the task of testing the actual vulnerability of business systems. The imaginary information security team should also include the Security Developer (28%), specialized in the development of security solutions, and the Machine Learning Specialist (19%), who prepares and controls security tools capable of dealing with possible threats automatically and cognitively in real time.

Moving on to privacy, which will be increasingly important given the forthcoming full application of the general regulation on data protection, is the DPO - Data Protection Officer, whose task is to facilitate compliance by organizations with the provisions of the GDPR. Overall, 28% of the sample has included in the workforce or collaborates with a DPO: if in 15% of companies the figure is formalized and in 10% is an informal presence, more than half of the sample (57%) states that they intend to introduce this figure in the company in the near future.

... but SMEs remain vulnerable! In fact, if we analyze the scenario in SMEs, things change radically. While in medium-sized businesses the person in charge of information security is covered by a real IT manager, in small and micro businesses it is the owner himself or the general manager who takes his place.

But what is worrying is the fact that in less than 30% of SMEs there is the figure of a security manager, while in 15% there is no figure to oversee the information security. And it works in particular for ISO and DPO, that are the two main job profiles linked with our project.

6.1.3 Information Security Labour Market in Italy

When applying the GDPR in micro, small and medium-sized enterprises, it must be remembered that the European Regulation is intended to protect the processing of personal data of natural persons regardless of the means used to carry out such processing. SMEs, as well as all other companies, have the obligation to comply with the General Data Protection Regulation (GDPR) that came into force in 2018. Privacy principles introduced (or strengthened) by the GDPR are still struggling to establish themselves in concrete application, despite the fact that we are finishing the third year of the new legislation.

The most obvious difficulties are those encountered by the figure of the Data Protection Officer (DPO), which, although already present in many organizations, is still struggling to take on the appearance outlined by the EU Regulation and the Privacy Guarantor, for various reasons that we will go into below. The brief considerations that follow, therefore, without claiming to be exhaustive and for the sole purpose of stimulating discussion on some operational aspects, are intended to give space to the "reverse" perspective of data controllers and data processors, as well as that of Data Protection Officers.

Very often, however, within the company you do not have the knowledge nor the tools to be able to comply, and the risk of incurring a strong penalty is high. The European Guarantor does not compromise on the incorrect processing of personal data and can sanction the company with very high fines. Here, then, it is necessary to adapt as soon as possible, relying on expert consultants and putting in order what are the internal processes of personal data management.

Below we have indicated the initial Checklist to follow to make yourself GDPR compliant: a first step towards full compliance.

1. Understand what "Personal Data" is.

Personal data is information that identifies or makes identifiable, directly or indirectly, a natural person and that can provide information about their characteristics, habits, lifestyle, personal relationships, health status, economic situation, etc. In particular:

a) data that allow direct identification - such as personal data (for example: first and last name), images, etc. - and data that allow indirect identification - such as an identification number (e.g. tax code, IP address, license plate number);

b) data falling into particular categories: these are the so-called "sensitive" data, i.e., those revealing racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, relating to health or sexual life. Regulation (EU) 2016/679 (Article 9) also included in the notion genetic data, biometric data and data relating to sexual orientation;

c) data relating to criminal convictions and offences: this is so-called "judicial" data, i.e., data that may reveal the existence of certain judicial measures subject to

registration in the criminal record (for example, final criminal convictions, conditional release, prohibition or obligation to stay, alternative measures to imprisonment) or the quality of defendant or suspect. Regulation (EU) 2016/679 (Article 10) includes in this notion data relating to criminal convictions and offences or related security measures.

d) With the evolution of new technologies, other personal data have taken on a significant role, such as those related to electronic communications (via the Internet or telephone) and those that allow geo-location, providing information on places frequented and movements.

Does the data you have fall into these categories?

2. Verify all your customer data: Where does your customer data come from and who do you share it with? Record everything in an organized and systematic way.
3. Review and refine your Privacy Policy: What are your current privacy policies, notices and disclaimers? Refine them to comply with GDPR rules.
4. Understand what "Personal Rights" are and make sure you comply with them

The GDPR guarantees the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights relating to automated decision making and profiling.

The Italian Data Protection Authority (Garante per la protezione dei dati personali) is an independent administrative authority established by the so-called privacy law (Law No. 675 of 31 December 1996) and regulated subsequently by the Personal Data Protection Code (Marcella 2003) as amended by Legislative Decree No. 101 of 10 August 2018, which also established that the Italian DPA is the supervisory authority responsible for monitoring application of the General Data Protection Regulation (pursuant to Article 51 of Regulation No. 2016/679, European Union 2016).

6.2 Institutional Landscape

See Annex II to this document for a concise overview.

6.2.1 Stakeholder Analysis

Several stakeholders have been identified with a strong interest in the work of the project, including chambers of commerce, training centres and regional authorities. There are both regional and national associations that represent i.e. IT and data protection experts. There are also some private organizations, with many years of experience with small businesses and their training needs. Generally, on the regional levels public actors are very active in regulating education.

Concerning the implementation and dissemination of project contents especially the specific office at Veneto Region premises (training and labour department) that is running the “regional repertory for professional standards and qualifications”)is interesting to sustain future communicaitons. This is the right body the Italian / regional implementation plan.

6.2.2 National Certification Systems

The National Qualification Framework (NQF) is the tool that describes all qualifications awarded within the national system of competence certification. The NQF refers national qualifications to the European Qualification Framework (EQF) in order to coordinate the national qualifications system with those of other countries. The purpose of the NQF is therefore to coordinate all the various systems that make up the entire public lifelong learning offer and that award qualifications.

The Ministry of Education and the Ministry of Labour developed the National Qualifications Framework as described in the Interministerial Decree of January 8, 2018. On December 20, 2012, the State/Regions Conference had sanctioned the agreement on the first referencing report of the Italian qualifications system to the European Qualifications Framework for lifelong learning (EQF). In 2015, the Ministry of Labour and the Ministry of Education had signed an agreement on the reference framework to the EQF of the qualifications issued within the regional vocational education and training (VET) system.

At national level, it has been published in the Official Gazette no. 13 of January 18, 2021 the Decree of January 5, 2021 of adoption of the Guidelines that make the National System of Certification of Competencies operational. The Guidelines are of strategic importance in that they represent the measure that makes the National System for the certification of skills operative, as per article 4, paragraph 58, of Law 28 June 2012, no. 92 and the aforementioned Legislative Decree 16 January 2013, no. 13, being part of the broader national process for the individual right to lifelong learning. In this context, the recognition and certification of skills acquired by the individual in formal, non-formal and informal contexts, together with the creation of territorial

networks and the creation of the single information backbone through the interoperability of existing central and territorial databases, are crucial to encourage and support a concrete increase in the participation of people in training, as well as a spendability of skills acquired in informal and non-formal contexts within the labor market.

The implementation of services for the identification and validation and certification of competences, in the regulations and policies, constitutes an essential strategic lever for the raising of levels of qualification and employability, for the competitiveness and productivity of businesses and professions and for the modernization and effectiveness of services and active labour policy measures.

The services of identification and validation and certification of competences will also be an important factor of innovation of the educational and training systems, favoring the personalization of learning in contrast to failure and dispersion and facilitating the transitions from study to work through a planning of the educational and training offer enriched and integrated by the contribution of a wider range of subjects, such as, for example, businesses and professional associations, the bodies that express the bilaterality or voluntary and third sector organizations.

At regional level, the Veneto Region has started a few years ago the construction of a Veneto system of validation of skills acquired by people. On December 28, 2012 were approved the Guidelines for the validation of skills acquired in non-formal and informal contexts. This document outlines the characteristics of the services to be offered to citizens. To date, useful tools for the recognition of skills have been perfected: the individual dossier of evidence of skills acquired and the certificate of learning outcomes acquired.

The guidelines foresee the activation of procedures and devices also for the validation of competencies. The two tools are the direct result of the experimentation coordinated by the Employment Section within the ESF system action Axis IV Human Capital (Pretto 2009). The Dossier and the certificate are already in use since 2011 within the services offered to workers who are beneficiaries of active policy interventions. The guidelines provide for the extension of their application also within the apprenticeship system.

During 2015, the construction of the Regional Repertoire of Professional Standards (RRSP) was started, which proposes a list of professional profiles significant for the territorial labour market and described by competencies to facilitate the shared representation of the skills required and recognized by the labor market. The competencies that make up the RRSP are technical-professional competencies, that is, referable to recognized and recognizable activities and results. The RRSP intends to contribute to describing the competence needs of the professions, to better balance the offer of professional training courses and the needs of the labour market and to contribute more and more to the process of integration between education, training and work at the service of citizens.

In this way, the RRSP intends to be a reference tool for:

- Identify skills gaps and deepen the analysis of skills needs with both companies and individuals
- Support guidance services and build personal career projects based on skills
- Realize services of matching demand-supply of skills
- Designing training paths, including internships, aimed at the acquisition of specific skills
- Validate skills acquired in non-formal and informal learning contexts
- Certify skills acquired in non-formal and informal learning contexts.

In the case of the last three services, the use of the Directory is part of a more regulated context, in which the use of the Directory and the competencies must be carried out in accordance with specific rules and methods.

Validating and Transparency Tools in Italy

The validation and transparency tools in Italy are based on LEGISLATIVE DECREE January 16, 2013, n. 13, “Definition of general rules and essential levels of services for the identification and validation of non-formal and informal learning and minimum service standards of the national system of certification of competences”.

The Italian Republic, in the context of public policies of education, training, work, competitiveness, active citizenship and welfare, promotes welfare, promotes lifelong learning as a right of the person and ensures person's right and ensures equal opportunities for everyone to recognize and valorisation of the competences however acquired in agreement with the aptitudes and individual choices and in a personal perspective, civic, social and occupational perspective.

In order to promote the growth and the valorisation of the cultural and professional patrimony acquired by the person in order to promote the growth and enhancement of the cultural and professional heritage acquired by the person in his or her life, study and work history, guaranteeing its recognition, transparency and spending.

recognition, transparency and usability, this legislative decree defines the general rules legislative decree defines the general norms and the essential levels of the essential levels of performance for the identification and validation of non-formal and informal learning and the minimum service standards of the service of the national system of certification of competences, referring to the areas of respective competence of the State, the regions and autonomous provinces of Trento and Bolzano, even in terms of function of recognition in terms of training credits in key European European key.

For the purposes and to the effects of the provisions of this Legislative Decree shall mean:

a) "lifelong learning" means any activity undertaken by a person in a formal, non-formal and informal way, in the various stages of life, in order to improve knowledge, skills and competences, in a perspective of competencies, in a perspective of personal, civic, social and occupational growth;
b) "formal learning": learning that takes place in the education and training system and in universities and institutions of high of high artistic, musical and dance training, and which ends with the with the achievement of a degree or qualification or professional vocational diploma, also achieved in apprenticeship, or a recognized certification, in accordance with current legislation on the subject of school and university regulations;
c) "non-formal learning": learning characterized by a person's intentional choice, which takes place outside of the systems of the systems indicated at letter b), in any organization that pursues educational and educational and training purposes, including voluntary work, national civil service and the national civil service and the private social sector and in businesses;
d) "informal learning": learning that, even without an irrespective of an intentional choice, takes place in the performance of carrying out, by each person, of activities' in the situations of of daily life and in the interactions that take place in it, within the context of work, family and leisure;
e) "competence": proven ability 'to use, in situations of work, study, or professional and personal development, a structured set of knowledge and personal development, a structured set of knowledge and skills acquired in formal, non-formal or informal learning contexts; and informal;
f) "titular public body": public administration, central, regional and autonomous provinces responsible, by law, for the regulation of regulation of services of identification and validation and certification of competences. Specifically, the following are to be understood titular public bodies
    1) the Ministry of Education, Universities and Research research, in the field of identification and validation and certification of competences of competences referred to the qualifications of the school and university system and university system;
    2) the regions and autonomous provinces of Trento and Bolzano, in the field of identification and validation and certification of competences competences referred to qualifications issued in the context of their respective competences;
    3) the Ministry of Labour and Social Policies, in relation to identification and validation and certification of competences the Ministry of Labour and Social Policies, with regard to the identification and validation and certification of competences referred to organized in orders or colleges, except for those in any case pertaining to the competent authorities as per point 4 below;
    4) the Ministry for Economic Development and the other competent authorities pursuant to competent authorities pursuant to article 5 of Legislative Decree no. 206 of 9 November 2007, n. 206, on the identification and validation and certification of competences certification of competences referred to qualifications of professions regulated under the same decree;

g) "entitled body": subject, public or private, including chambers of chambers of commerce, industry, handicrafts and agriculture, authorized or accredited by the titular public body, or designated by state or regional law, including educational institutions, universities scholastic institutions, universities and institutions of higher education artistic training, music and dance, to provide all or part of the services services of identification and validation and certification of competences competences, in relation to the areas of ownership 'referred to in paragraph letter f);
h) "Italian national accreditation body" means a national accreditation body national accreditation body designated by Italy in the implementation of (EC) (European Union 2008);
i) "Identification and validation of competences" means the process leading to the recognition by the general rules, the essential levels of services and the minimum standards services and the minimum standards referred to in this decree, of the competences skills acquired by the person in a non-formal or informal context informal context. For the purposes of identifying the skills are also considered those acquired in formal contexts. The validation of competences can be followed by the certification of skills or ends with the issuance of a document of validation of validation in accordance with the minimum standards referred to in Article 6;
j) "qualification": an education and training qualification, including that of including that of vocational education and training, or of professional qualification issued by a titular public body, in accordance with in accordance with the general rules, the essential levels of services and the minimum standards of essential levels of performance and minimum standards referred to in the decree;
k) "National system of certification of competences": the set of services for the identification and validation and validation and certification of competences provided in compliance with general norms, the essential levels of services and the minimum standards minimum standards referred to in the present law.

National Competence Certification System

In line with European Union guidelines, the following are subject to identification and validation and certification of competences acquired by the person in formal, non-formal or informal contexts, whose possession is demonstrable through feedback and evidence defined in compliance with the guidelines referred to in paragraph 5.
The entitled body can identify and validate or certify skills related to the qualifications included, for their respective areas of ownership 'referred to in Article 2, paragraph 1, letter f), in repertoires codified at national or regional level according to the criteria of referencing to the European Qualifications Framework, or to parts of qualifications up to the total number of competencies constituting the entire qualification.
Without prejudice to the provisions of present decree, with regard to the universities' reference is made to Article 14, paragraph 2 of Law 30 December 2010, n. 240.
Only the competences referred to qualifications of repertoires included in the national repertoire of Article 8, without prejudice to the provisions of Article 11.

The national system of certification of competences operates in compliance with the following principles

a) the identification and validation and certification of the competences are based on the explicit request of the person and on the enhancement of its heritage of life experiences, study and work. of work. Centrality 'of the person and voluntary process require the guarantee, for all citizens, of the principles of Simplicity, accessibility, transparency, objectivity, traceability, confidentiality of service, methodological correctness, completeness, fairness and non-discrimination;
b) the validation documents and certificates issued respectively at the conclusion of the identification and validation and certification of skills are public acts, without prejudice to the value of qualifications provided for by law in force;
c) the public bodies responsible for the national system of certification of competences, in regulating and organizing the services in accordance with this decree, operate autonomously, according to the principle of subsidiarity according to the principle of subsidiarity 'vertical and horizontal and in respect of respect for the autonomy of educational institutions and the university', organically within the unitary framework of interinstitutional coordination and in dialogue interinstitutional coordination and dialogue with the economic and social economic and social partnership;
d) the connection and the mutuality of services for the identification and validation and certification of skills is based on the full implementation of the realization of the single information backbone referred to in Article 4, paragraph 51 of Law June 28, 2012, n. 92, through the progressive interoperability 'of existing central and territorial databases and the establishment of the national repertory of education and training titles and training and professional qualifications;
e) the reliability of the national system of certification of skills is based on a shared and progressive competences is based on a shared and progressive system of indicators, tools and quality standards throughout the national territory national territory.

Verification of compliance with the levels of service of the national system certification of competences, in respect of the principles of principles of third party and independence, provides a technical committee national, established by this decree without new or increased burdens on the public finance, chaired by representatives of the Ministry of Labour and Social Policies and the Ministry of Education of education, university and research, made up of representatives of the representatives of the Ministry for Public Administration and and simplification, the Ministry for Economic Development, the Ministry of Economy and Finance and of the administrations public administrations, central, regional and autonomous provinces of Trento and of Bolzano in their capacity as public bodies in accordance with the this legislative decree. Within thirty days of the entry into force entry into force of the present decree, the member administrations designate their technical representatives within the committee.
The members of the committee is not 'paid any compensation, emolument, indemnity' or reimbursement of expenses. In the exercise of its duties, the committee proposes

the adoption of appropriate guidelines for the the inter-operability of the titular public agencies and the relative functions primarily aimed

a) the identification of indicators, thresholds and methods of control, evaluation and verification of the minimum standards referred to in this decree, including for the purposes of the essential levels of performance and guarantee of services;
b) to the definition of the criteria for the implementation of the national repertoire of which to the article 8, also in the perspective of the European system of credits for education and professional training vocational training, and for periodic updating, to be carried out at least every three years;
c) the progressive implementation and functional connection of the single information backbone referred to in article 4, paragraph 51, of law no. 92 of Law no. 92 of June 28, 2012.

The committee organises periodic meetings with the economic and social partners in order to guarantee and social partners in order to guarantee information and participation in the phases of elaboration of the guidelines, also at the request of the parties themselves.

The guidelines referred to in paragraph 5 are adopted by decree of the Minister of labour and social policies, in consultation with the Minister of Education, Universities and Research, the Minister of Public Administration and Minister for Public Administration and Simplification and the Minister of Minister for the Economy and Finance, having consulted the Minister for Economic development, after agreement with the Unified Conference pursuant to Article 8 of Legislative Decree 28 August 1997, n. 281, and after consultation with the economic and social partners.

TeBelSi - The recognition process of TeBelSi Training as non-formal education in Italy

The entry into force on May 25, 2018 of the European Regulation for the Protection of Personal Data (GDPR - General Data Protection Regulation) has made even more fundamental the obligation for entities that carry out the processing of other people's data to adopt technical organizational security measures and precautions to protect the dissemination of sensitive data by protecting them from possible illicit acts. The core philosophy of the new GDPR is accountability (or responsibility) for all stages of processing; this involves the adoption of tools and solutions to ensure not only the protection of data, but also the control, verification and analysis of procedures. In order to do this, the company must have employees trained in the principles of PRIVACY and the company procedures in place.

The Regulation does not specify in detail what kind of courses must be carried out (as e.g. provides for the legislation on safety at work), but the obligation derives from Articles 29, 32 and 39 of the EU Regulation 2016/679 (European Union 2016). As provided for in Article 29 of the Regulation, the controller, or anyone acting under its authority or that of the controller, who has access to personal data may not process

such data unless instructed to do so by the controller, unless required to do so by Union or Member State law.

Training obligations are introduced by art. 39.1.b of the Regulation, which provides, among the tasks of the DPO, to "monitor compliance [...] with the policies of the controller or processor on the protection of personal data, including [...] awareness raising and training of staff involved in processing and related control activities", and furthermore, art. 32.4 of the Regulation provides that "anyone who has access to personal data shall not process such data unless instructed to do so by the controller".

Companies and Public Administrations, therefore, must implement training processes that meet the requirements of Security Measures: testable, verifiable and assessable for anyone who handles personal data. In case of violation of articles 29 and 39 (training obligation), administrative fines will be applied that could be significant.

The PRIVACY course (recommended at least 2 hours of training) aims to provide the main notions to educate employees and collaborators on the topic of personal data protection under the EU Regulation 2016/679 (GDPR) (European Union 2016), covering in particular the following topics:

- Principles of Regulation 2016/679
- Actors in the processing of personal data
- Appointments of figures in relation to the organizational structure
- Risk-based approach to processing
- Compliance with the procedures and security measures adopted
- GDPR documents

To maintain compliance with the GDPR PRIVACY is expected to update at least every three years of training for all employees who handle data.

The recognition of TeBeISi Training by professional associations

In the list of stakeholders, we also mentioned “APCO”, that is the italian association for management consultants. APCO organizes, several times, courses in different topics and, at the end of the path, they recognize the “training credits” following the Italian legislation (Law nr. 4 / 2013).

The recognition of TeBeISi Training as formal education in Italy at University Level

Also in Italy, like in the other project country, our TeBeISi contents can be recognized (as part of the study programme) based on the ECTS System, in full University or Applied University in the framework of existing Bachelor or Master Programme.

7 Implications for the Project

7.1 Summary of National Background Information

Information security in Germany demands great efforts from firms and employees in order to tackle the skills shortage. Meanwhile broad study programs exist concerning mainly IT-security, especially on Masters level at Technical Universities, low-threshold offers remain scarce. The Chamber of Industry and Commerce provides for the opportunity to engage with IT Security as Coordinator or Technician on a EQF 5 level, either after completing a corresponding VET program or after having accrued 3 years of relevant work experience. Similar entry requirements can be noted for the majority of certification programs, which mainly ab at further qualifying existing information security personnel. As a result, 2 key points can be highlighted: 1) specific information security offerings remain scarce, especially in the VET sector, and that continuing education programs are not tailored towards the inclusion of workers without pre-requisites in the labour market. 2) Partial certification programs are being developed for VET in Germany, however, non are available for courses close to the topics of information security. Similarly (and consequently), there are no partial qualification possibilities.

A similar picture can be painted for Austria, where the “Second Chance Education System” provides for manifold possibilities of re- and upskilling in the context of adult education. Meanwhile the chamber of commerce plays a crucial part in the organization of VET and poses therefore a key player in the proposition of future partial qualification programmes; validation of prior learning is still in development and currently no concrete programmes in action exist to refer to. Nonetheless, a clear connector between information security, data protection and educational needs is missing. Promising actors and initiatives to foster especially projects with a focus on SMEs are available.

Lithuania provides a much more homogenous field of actors with a stronger concentration of interests. Meanwhile hybrid education, as a result of collaborations between VET schools and colleges exist, actors with a clear interest in piloting and certifiying courses have been identified.

Poland disposes of a unique feature in its labour market, the Integrated Qualification System. This feature allows for the integration of new qualification which emerge on the free market into the official polish education system. Therefore, the system inherently welcomes the proposal of new qualifications – be it in part or full. Due to the strong digital focus of the economy, several players and organizations have been identified with a strong interest in the work of the project. These are either specifically focused on the work of SMEs or on the general constitution of IT education in Poland. Due to the system, certification is encourages by various certification providers.

Finally, the Italian competence recognition system is quite complex: there are general guidelines that come from Ministry, national agency and, ultimately, the single regions are dealing with local companies. There is strong focus on regional actors concerning the provision of education and a national focus concerning the organization of Information Security Experts and Associations.

Considering these aspects, it becomes apparent that re- and upskilling through VET provides valuable opportunities to provide the labour market with duly sought skills. In the realm of needs of SMEs, the advantages for partial certification and qualification become more apparent, as training in specific fields of information security would allow firms to educate their employees more economically, as the own specific need can be taken into account when choosing a teaching program.

7.2 Conclusion and Suggestions

In light of the findings from the stakeholder analysis and the country reports, it becomes clear that plenty of potential exist for the member states to learn from other educational systems and to thereby close gaps in the educational market. It can be noted that every country disposes of particular advantages, but also disadvantages.

For the TeBeISi project, the most important finding is the greater use of EQF 5, which is true especially for western European countries. The bridge between VET and HE via short cycle studies provides many opportunity to address competence needs in the realm of information security and data protection. Holders of level 5 qualifications have a comprehensive theoretical basis in their field of work or learning and are able to design projects independently as well as find the solution to different problems also in unpredictable contexts. They also have the ability to work creatively on their own and to think critically. Holders of level 5 qualifications can carry out the tasks associated with the activities on their own responsibility. They can carry out the tasks associated with these activities on their own responsibility. Furthermore, they can lead work teams and take responsibility for timely and result-oriented implementation (OEAD 2021a).

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 3: EQF Level 5 Learning Outcomes - Knowledge - Skills - Competences

Source: European Commission (2008)

To achieve an adaptive and flexible curriculum, learning modules shall be developed which are additive and holistically reflect the set of competences that SMEs might need. In a second step, a tool for better orientation will be developed to help SME owner and learners to determine which contents they should prioritize.

7.2.1 Learning Modules

From the findings derived above, several points can be taken which are to be considered for the development of the learning modules: 1) the learning-outcome oriented definition of learning units 2) the appropriate scope for the needs of SMEs and 3) adaptability for flexible implementation across several educational systems and geared towards individual needs. Consequently, the development of a modularized curriculum which can be implemented in a micro-credentialised environment in order to ensure recognition and certification for learning shall be achieved in the partner countries. Due to the large need of flexibility and customization of individual SMEs needs, the curriculum will be sidelined with a self-assessment tool to provide learners and SME owners some guidance concerning their individual necessary to learn modules.

The content of the learning modules will be derived from the expert Interviews, the occupational profiles, literature research and certification contents. From these sources, jointly exhaustive and mutually exclusive learning fields will be derived and adequate levels of competences for EQF 5 defined. Formulations will be drawn from the ESCO database to ensure transferability of the competence sets. If need be, new competences will be suggested if gaps are being discovered. The competence sets will draw on technical, social, methodological and personal competences and thereby reflect an holistic approach to action oriented competence definition.

7.2.2 Self-Assessment

The project team came to the conclusion that the learning units can pose a new barrier of complexity towards SMEs, as they might not be aware of what they need and which contents they should look for. To this end, a supportive questionnaire helps SMEs to determine their individual need and to help choose the right learning modules.

7.2.3 Research Report

The results of the questionnaire and some additional findings concerning the modules developed will be included and evaluated in the IO 6 research report. The report will not only provide insights into the need of SMEs and existing solution approaches practiced in business reality, but also draw recommendations and future action needs to provide practitioners, educational providers and learners with recommendations for the future.

8 Feedback from stakeholders: Curriculum + Self-evaluation (All Partners)

8.1 Background information Steering Committee (Function, Qualification, Field of Work, Anonymous Code).

Germany

ID	Function / Job Role	Employer (SME, ministry, NGO etc.)	Qualification, Job experience
DE_SC_01	Scientific Employee	NGO	PhD Social Science
DE_SC_02	Referee for Education and Training	Chamber of Commerce	MSc Business Administration
DE_SC_03	Head of Information Security	SME	MSc., 3 Years job experience

Austria

In the former project "INSEMOT SME - Information Security Modular Training for SME", coordinated by Hafelekar, we worked with several experts in the field. The following three experts have agreed to support us in the TeBeISi project as well.

Our Steering Group is composed of three experts who are Managing Directors in SMEs and MEs, who have been dealing with the topic of information security and data protection for a long time.

ID	Function / Job Role	Employer (SME, ministry, NGO etc.)	Qualification, Job experience
AT_SC_01	**Managing Director of a**	**Medium-sized enterprise (40 members of staff)**	The internet agency stands for innovative IT projects in Austria, Italy and Germany. The portfolio ranges from consulting, conception and design of web projects to programming of complex applications. Since web hosting is also offered and sensitive data is processed, the areas of information security and data protection are highly relevant.
AT_SC_02	**Managing Director of a**	**Small enterprise (12 members of staff including network partners)**	This company offers advice in the fields of tax consultancy, legal advice in the ICT sector and organisational development. They advise clients specifically in the area of data protection. Since highly sensitive data is processed in the company, information security is an important topic internally.

AT_SC_03	**Managing Director of a**	**Micro enterprise (3 members of staff & freelancers)**	This company has been developing efficient web solutions for 20 years, from concept to graphics and programming to hosting. Image, text, video and database functionality play a major role. The company also handles business for large companies. So, both areas, information security and data protection play an important role.

Method of the interviews

Due to the current pandemic situation, personal meetings were unfortunately not possible. In addition, small companies in particular are currently under pressure to be able to maintain their ongoing business, organise the situation with short-time work and work on customer loyalty.

Hafelekar therefore chose the following setting:

- Several telephone conversations with stakeholders to encourage them to participate in the TeBeISi project.
- In a second step, we forwarded the project description and the documents on the planned curriculum.
- Afterwards, an appointment was made for team meetings to go through the questionnaire. Two MS team meetings took place at the end of February and the third at the beginning of March.

Poland

ID	Function / Job Role	Employer (SME, ministry, NGO etc.)	Qualification, Job experience
POL _SC_01	Management Board Advisor	SME	
POL _SC_02	MSc, Lecturer in Information Technology	Higher Education entity	
POL _SC_03	Entrepreneur in the development services industry, President of the Management Board of BRITISH CENTRE sp. z o.o. Vice President of the Association of Owners, Presidents and Directors of Companies Club 500-Lodz Member of the Board of the Chamber of Commerce and Industry in Łódź Chairwoman of the Council of the Polish Chamber of Training Companies Chairwoman of the Committee on Vocational Education of the National Chamber of Commerce	SME, Association, Chamber of Commerce[SR1]	

Italy

Our Steering Group is composed of three experts who are Managing Directors in SMEs, training companies and regional offices, who have been dealing with, in general, the (part) certification processes and sometimes in the topic of information security and data protection for a middle/long time.

ID - code	Function / Job Role	Employer (SME, ministry, NGO etc.)	Qualification, Job experience
IT_SC_01	**Training department and EU funds - Director**	**Training centre (45 members of staff + 150 external trainers and consultants)**	The training centre has been founded in 1956; it is a regional body that offers several courses for a wide range of SMEs needs. It offers course free of charge (founded by ESF – European Social Funds) but also through a catalogue.
IT_SC_02	**Managing Director**	**Small enterprise (15 members of staff including network partners)**	This company has been founded in 1998, and it offers training and consultancy services. They advise clients specifically in the area of training for NGO and associations. The company also set up some platforms for the (part) certification for example in the field of tourism and manufacturing.
IT_SC_03	**External Manager**	**Public labour agency (480 members of staff, plus thousands of external experts)**	It is a public body, the regional labour agency. It offers several services like: job basic information and orientation; local agencies for un-employed people; link with the regional repository for professional profiles, etc.

Method of the interviews

Due to the current pandemic situation, personal meetings were unfortunately not possible. In addition, SMEs in particular are currently under pressure to be able to maintain their ongoing business, organise the situation with short-time work and work on customer loyalty.

CDPZ therefore chose the following setting:

- Several telephone conversations with stakeholders to encourage them to participate in the TeBeISi project.
- In a second step, we forwarded the project description and the documents on the planned curriculum.

- Afterwards, an appointment was made for Skype meetings to go through the questionnaire. One MS Skype meeting took place at the end of January; and the second and third at the end of February.

Lithuania[SR2]

ID	Function / Job Role	Employer (SME, ministry, NGO etc.)	Qualification, Job experience
LT_SC_01	Professor of University	HEI	Expert in information security and personal date protection
LT_SC_02	Educator	NVO	Expert in adult education
LT_SC_03	Lawyer	Privat organization	Expert in law

8.2 How does the demand for TeBelSi project results look like in the country?

Germany

Among the steering group members, the sentiment was shared that there is lack of awareness for information security both among firms and among employees. Meanwhile more and more company leaders embrace the necessity to invest time and personnel into a certification of their firm (i.e., ISMS), the difficulty to find suitable personnel remains a difficult problem to solve.

One candidate described the situation as follows:

“We offer certification courses which allow firms to send employees with very little experience in information security. These employees receive the opportunity to find a new role within their firm and acquire new skills. The firm literally invests into them. However, we have been reported that after a couple of months, it happens that employees are not satisfied with their job, and they happen to leave the firm. The firm not only lost financial resources and time, but also an employee throughout this process”. (DE_SC_01)

This story is supported by the impression by another participant: “If I were to choose between candidates with good technical skills or candidates with good social skills, I would prefer the one with the better social skills. Attitude is the most important factor in this field, all the rest you can teach.” (DE_SC_03)

Topic	DE_SC_01	DE_SC_02	DE_SC_03
Is a project on data protection and information security needed?	Definitely yes! What we need is to raise awareness more generally, information security does not begin in the office! The European public needs to be made aware and sensitized for threads in the cyber realm!	From my perspective, we need information to be more easily available among SMEs. We have many firms that engage in our information activities, but we need to provide firms with the ability to look after themselves.	Our firm is very well off concerning the need of new employees. The firm looked out for qualified personell from a very early point in time and managed to secure valuable assets. But we could need some support, especially the awareness of all employees is a big challenge.
What are your specific needs?	We have many members that seek for practicable solutions below a ISO2700X certification. We developed such a solution ourselves, but I think many firms have difficulties to understand the advantage of a coherent management system. To persuade more firms would be a big help!	We experience both a strong and a very weak interest – that is, we have some few firms with specific demand, but the majority remains uninterested. I think if we were to address this topic, we need some very basic, low-threshold informative sessions. The firms I am referring to are diverse, but in my opinion very active and innovative in what they do and how they do it. If we don't find a solution, probably someone else will.	Currently, we are in the auditing process to get ISO27001 certified. This is a lot of work, and many very detailed and informed processes need to be aligned and documented. It would be great to have personnel available to support in this regard – doing more basic work, which takes up a lot of time and energy. But generally, this period will pass and we are otherwise well prepared.
Balance internal training needs with external offers?	There is a great amount of offers on the market. What is best for my company? I think more transparency about useful and effective training would be good.	We offer some counselling ourselves. But we don't offer certifications. What we see is needed are offers for very specific questions – and very basic and introductory offers. I feel like many firms get the idea of "this sounds fancy – but I am only a small company. Surely this doesn't concern me. I don't even have sensitive information!". External offers can only do so much – when firms actually have interest.	Here in the region we have some very experienced service providers which can support in the documentation, counsel for auditing or provide external data protection officers. In the long run, it would be cheaper for firms to have own personnel to do that, but I figure that especially for the smaller firms, there is not enough that needs to be done to feasibly fill an entire position.
What do you think about	The curriculum is detailed and touches on all	Generally, the idea of the curriculum is very interesting. We talks about implementing	The idea is great! We need people that learn how the work is done on a very low

the TeBelSi Curriculum?	important aspects of the work of an information security expert in an SME. The most important part is to hammer away at perseverance and communication strategies, to motivate and to exert authority. I think this is covered adequately. Nonetheless, I figure that it might be a risk that these modules might be devalued by the persons choosing the topic and – again – will not be learned. So some sort of recommendation would be good.	some contents in a VET environment. Unfortunately, schedules are already very tight. It is further difficult to decide which units should be incorporated into the learning structure of different courses. We agree that this is a matter like health and safety, but we don't feel like these contents are necessarily appreciated by the firms where the pupils work – they don't always see the tangible benefit.	and routinised level – this would already help a lot! Of course, it would be great if these people received the opportunity to make further steps in their career building on the learned contents. But from a firms perspective, a first understanding and know-how is very attractive.
What would your desired job profile look like?	We need to attract people that truly understand and live the idea of informational independence and security. The objective should be that every European citizen is aware of misinformation and manipulation strategies, in a civic and in a corporate context. This would make the job much easier for firms. In the meanwhile, we need more people from non-IT backgrounds to close a communication bridge between the business units.	The idea of offering vocational training in data protection and information security is very innovative, and there are some initiatives in this direction ongoing in other chambers. But defining the scope of contents and, more importantly, finding acceptance on the market is a different story.	We are currently looking to improve our data stragtey and therefore also data protection professionals. These are very expensive. We know there are courses where students learn about corporate law, but data protection doesn't play a role in it. So we would appreciate of more legal fundamentals would be taught in universities, which would increase the employability significantly.

Would validation of prior learning make sense?	Yes, validation would make a lot of sense! I, for example, come from a completely different domain – from social sciences. And there are many experts like me who became very very motivated to engage in information security and improve and motivate firms to engage in their security. We need more discussion about this topic in the public sphere in general.	I know of several initiatives that implement validation strategies for prior learning in plenty of vocational domains. But we encounter severe difficulties of acceptance: many firms argue that the quality of the assessment is too low and that a short assessment can never be regarded as equivalent to a three year training. So there are growing pains and trust in the validation systems needs to be very high in order to work effectively. But if that was the case: yes, I think this would help many people on the labour market.	From what I understand – yes. I know many people with significant experience. As of now, they will find a job if they wanted to either way, firms take what they can get, and if they receive the impression that you know what you are talking about or have interesting projects done in the past you will get an opportunity somewhere. But I am not sure if this will change. If, in the future, more personnel will have qualifications, also lateral entrants will need some sort of proof I think.
Would you accept an employee who has no formal education in both fields?	This is a difficult question. Most importantly, we need to make sure that the motivation exists to live and practice information security.	We rarely observe the hiring politics among the firms, but we realize that in some areas, especially IT or technology driven fields, interest and prior work experience matter more than a piece of paper. But I am unsure how it is possible for people to convey their experience to even get a job interview.	Yes, I would. Of course, for data protection there are legal obligations, especially if you want an employee who is capable to actively practice law. But otherwise, it is important that people get what we are talking about, that they understand how my firm works and that they show the ability to interact in our environment.

Austria

Provisions on Managing Director Liability (UGB, GmbH Act) in Austria:

It follows from the provisions of the above-mentioned laws that the responsibility for information security always remains with the company management. Security-relevant IT tasks can be delegated to individual employees within the framework of formal specifications (e.g., an IT security policy). Nevertheless, the management bears the ultimate responsibility, especially for compliance with legal regulations. The same applies to compliance with the GDPR, i.e., data protection. We would like to point out once again that managing directors of companies in Austria bear the ultimate responsibility with regard to information security and data protection. This should be kept in mind when reading the answers of our Steering Committee.

Topic	AT-SC-01 – Medium-sized enterprise	AT-SC-02 – Small enterprise	AT-SC-03 – Micro enterprise
How important are IS and DP in your company?	Yes, both internally and externally, as many clients entrust us with their data and we need to protect our system.	In our business, both fields have the highest priority. We even consult clients in both fields and we know the difficulties of implementing.	We know how important this is, and as Managing Director I am aware of my responsibility. Nevertheless our resources are limited.
What are your specific needs?	Find employees who can act as an interface between management and staff. We cannot create a full-time position for IS and DP. So, we need staff who are interested in the topics but also contribute productively (e.g., programming area).	We do internal training to keep staff up to date in both fields. But sometimes we don't have the time, because the staff also have to do their main tasks. With our company size, it is not possible to hire one person for IS/DP. Staff costs are very high in Austria.	We do our best to stay up to date. The responsibility for IS/DP lies with the Managing Director. He lives off the "creativity" of his staff, who are not interested in these issues.
Balance internal training needs with external offers?	We have already invested money in external training, but then this trained person lost patience. It is difficult to constantly point out the necessary safety measures to the other employees. In the end, I as the manager have to undertake this task again.	External trainings are very expensive. If there was a cheaper offer, that would be very good for us. Nevertheless, in my function as the manager of our firm, I will always have the ultimate responsibility for Information Security and Data Protection.	Offers on the market are too expensive. Would be great to attend a training for free or low cost. In our case I would attend such a training.
What do you think about the TeBelSi Curriculum?	Although we have only received the brief descriptions, it seems very comprehensive and covers all the important areas of IS and DP. For a relatively short training of 2 to 3 weeks, many - perhaps too many - topics are covered. What I like is that people's aptitude (via soft skills) is addressed. We learned that not everyone can do this job. It is difficult to mediate between management and staff and to constantly point out the necessary safety measures.	At first glance, the content seems very good to me. It is important to me that the legal situation in Austria is sufficiently addressed. I could imagine taking part in such a training myself and also motivating interested employees to do so.	I would love to take part in such a training. I get my information on IS and DP mainly from the Chamber of Commerce. Free workshops on individual topics are also offered from time to time. It appeals to me that you can complete a relatively

	In the interview you asked me about the "level of autonomy": I recommend being careful here, because people in this job also have to know their limits. The ultimate responsibility in both areas always lies with the management. Overall, such a course also seems very interesting to me for refreshing knowledge in both areas.	It is a pity that no piloting has taken place yet and that it is not yet possible to say exactly how long the training would take and how high the costs would be.	comprehensive training in a short time.
What would your desired job profile look like?	A kind of "IS/DP Expert" who is able to play a mediating role between management and staff. This would take a lot of pressure off me as the managing director. In addition to the professional qualifications in both areas, it is important to me that this person has a real interest in the topics and brings along the personal suitability.	We are too small to create an own position for a kind of “IS/DP Officer”. But such a training would allow us to train internal staff members who would like to work in this field part-time, in addition to their actual job. Using external experts who work for several companies seems too risky for us, as we are dealing with very confidential data.	Unfortunately, we cannot afford to create a separate position for this. It would be great to have kind of experts who offer their service on IS/DP for several firms, which would keep costs low.
Would validation of prior learning make sense?	YES A shortening of the training period would be desirable.	YES It is a pity that this is still very difficult in Austria.	YES Prior knowledge should be given much more attention.
Would you accept an employee who has no formal education in both fields?	YES As Managing Director, I constantly have to deal with IS and DP. So, I think I can judge in a very short time whether a person has a clue or not. More important to me than expertise is personal suitability for this job.	YES/NO But unfortunately, as I said, we cannot create a separate position for it.	YES/NO If I could afford a person in this position, I would pay more attention to the practical skills than to the formal degree.

Poland

Topic	PL_SC_01	PL_SC_02	PL_SC_03
Is a project on data protection and information security needed?	"It's hard to get any other answer than yes, needed. Many organisations of all sizes do not even recognise the scope that such an issue covers. It often consists of a possible attention to personal data, but it is a much broader area."	"Given that we now live in the information age, the issue of its security has become crucial in many areas of life, both in the private and business spheres. "	"The TeBelSi project fits perfectly into the current market needs. Small and medium-sized companies, which cannot afford to employ high-class specialists in this field, find it difficult to cope by sometimes using outsourcing. An alternative method would be to adequately train their own employees, although in a situation of pandemic and collapse of the service market, closed by government regulations, a significant barrier arises: lack of financial resources. The answer to this problem is to take advantage of training funded by the implementation of this and other similar projects."
Do you frequently encounter information/data security needs in small and medium-sized companies?	"While every organisation strives to protect its information, companies, especially smaller ones, lack a structured understanding of how to do so. There are so many solutions available today to assist business in this area that it is difficult to choose a solution that is tailored to your organisation."	"Data security needs are now a priority for many institutions and technology companies (and not only those in the IT industry). The trend of increasing interest in the topic can be observed, among others, as a result of changing legislation (e.g. RODO) as well as growing customer expectations and related security standards (e.g. ISO 27000). "	"Modern companies have had to change the way they operate overnight for reasons beyond their control and have moved many - if not most - of their management and workflow processes and organisation of work to the Internet. This raises new challenges in terms of data protection and information security. However, there are plenty of issues in this area that require supplementing the knowledge and skills of employees."
Is it easy to find expert staff in this area?	"I think I would ask the question differently. The market today is quite well supplied with	"It is hard to recruit experts in the area of data security because it is an interdisciplinary field, requiring thorough	"It is difficult to overestimate the usefulness of such activities, which in the first stage will make it possible

	various competences that can be acquired on business terms. But how do you source an expert who won't throw the baby out with the bathwater and block growing companies with their processes? I think the hardest thing is to get experienced experts who have been through information security incidents of various sizes and can offer adequate solutions."	knowledge not only from many IT areas, but also from non-technical ones (e.g. from the area of social psychology). Moreover, it is necessary to have broad industry experience and to be constantly up-to-date with trends and changes in the discussed area."	to estimate the needs in this area, and in the second stage will make it possible to satisfy them in the form of training. The market lacks specialists with an expert level of knowledge, and if they do appear, the expected remuneration exceeds the possibilities of medium-sized and especially small companies."
Should activities on strengthening staff capacity on data protection and information security be developed in the future?	"They should be developed, consolidated and reviewed."	"The security of data and information systems does not only depend on the degree of technological advancement and the implementation of appropriate processes in the organisation, but the knowledge and awareness of these aspects among employees are crucial. In this context, it is particularly important that they are properly trained and prepared for different scenarios and cases related to data protection and information security."	"Certainly the project has a developmental character, as it will not be easy to meet the market needs in this area. I am hugely pleased with this initiative, my company is keen to participate in the project and benefit from the needs survey and training. I am happy to recommend the same to other entrepreneurs."
Would certification / obtaining a training certificate by an employee matter to you?	"The certificate itself is an endorsement of the training. I would like to have a certificate accredited by an entity that defines information security standards."	"Certification helps to ensure that data protection and information security is understood and applied in line with current standards and market expectations, so it should be considered and chosen wherever possible."	

Italy

Topic	IT-SC-01 – Training centre	IT-SC-02 – Small enterprise	IT-SC-03 – Public labour agency
How important are IS and DP in your company?	Yes, both internally and externally, as many clients (SMEs that are demanding training courses) are still dealing with IS/DP issues.	In our business, both fields have the highest priority. We even consult clients in both fields and we know the difficulties of implementing.	We are a public body; so our priority is to ensure the certification and validation processes.
What are your specific needs?	During our courses for IS/DP managers, we understood that find employees who can act as an interface between management and staff is crucial. We can not create a full-time position for IS and DP, in the small businesses. So, we need staff who are interested in the topics but also with good level of basic knowledge in the three main professional profile areas (IT. Legal and governance)	We do internal training to keep staff up to date in both fields. But sometimes we don't have the time, because the staff also have to do their main tasks. With our company size, it is not possible to hire one person for IS/DP. Staff costs are very high in Italy, due to taxation.	We are managing thousands of data, as public agency. So, each department is dealing with IS/DP issues, at central (regional) and local (district) level. We should balance the internal knowledge (some workers are attending, constantly, courses) with the external experts contributions (like the DPO).
Balance internal training needs with external offers?	In 2018, we have already invested money in external training. But, in the end, I as the manager have to undertake this task again. Basically because the external expert does not know exactly our internal procedure.	External trainings are very expensive for micro and small businesses. If there was a cheaper offer, that would be very good for us. In any case, as the manager, I will always have the ultimate responsibility for Information Security and Data Protection.	We are a public office, so everything has been done through an external expert (DPO, Data Protection Officer). In general, offers on the market are too expensive. For small businesses, would be great to attend a training for free or low cost.
What do you think about the TeBelSi Curriculum?	Although we have only received the brief descriptions, it seems very comprehensive and covers all the important areas of IS and DP. As training centre, we could also offer it, free of charge (thanks to ESF – European Social Funds) or for	Although we have only received the brief descriptions, it seems very comprehensive and covers all the important areas of IS and DP. It could be also offered to Chambers of commerce and/or trade associations. So, a	Although we have only received the brief descriptions, it seems very comprehensive and covers all the important areas of IS and DP. It could be a good basis for the validation process, even if the duration should be better defined.

	payment through our catalogue. It could also became a sort of Master degree, if we could combine the three main elements (legal, ICT and governance) but in that case the target will became only the middle and big size companies.	bigger number of participants will strongly reduce the prices.	
What would your desired job profile look like?	A kind of "IS/DP Expert" who is able to play a mediating role between management and staff. So, soft skills and communication tools are crucial, above all for implementing the concrete solutions in the day by day work. For us, as training centre, the project is interesting for two reasons: a better market offer in term of courses for SMEs; a bigger offer in term of qualified experts on the IS/DP framework	We are too small to create an own position for a kind of “IS/DP Officer”. But such a training would allow us to train internal staff members who would like to work in this field part-time, in addition to their actual job. Moreover, the project is interesting in term of comparisation with other validation and certification processes, that we made in the last years.	As big public body, we have some workers that are dealing with IS/DP issues and, as external expert, a consultant who is supporting us as DPO – Data Protection Officer.
Would validation of prior learning make sense?	The right training period would be desirable.	It is a pity that this is still difficult in Italy.	Prior knowledge should be given much more attention.
Would you accept an employee who has no formal education in both fields?	Yes, as Managing Director, I constantly have to deal with IS and DP More important to me than expertise is personal suitability for this job.	Yes, but unfortunately, we cannot create a separate position for it (we are a small business).	Yes, I would pay more attention to the practical skills than to the formal degree.

Lithuania

8.3 Feasibility of self-assessment and curriculum

Across all countries, a positive sentiment regarding the implementation of the curriculum and the development of a self-assessment can be determined. Besides a general need for more flexible training opportunities, experts noted specifically the need for easier and more practice-oriented training. Specifically, the need to find personnel with strong interest and perseverance in the topics and the capability to interact productively with other people were mentioned.

Experts showed further interest in increased opportunities to educate own employees and to fill in positions with a double-hatted responsibility. All experts agreed that prior knowledge plays a pivotal role in the current hiring practice, even more so than formal qualifications. Nonetheless, some sort of certification possibility will facilitate the hiring process and, especially when more certified personnel is available on the market, provides equal opportunities to all employees, i.e.lateral entrants and native learners.

From a firms perspective, it became clear that filling several positions for information security and data protection in many cases represents a non-viable or less favoured option in comparison to the unification of both fields of responsibility. The unification would make sense from a functional perspective, as both domains are closely related, and an economic perspective, as several positions rapidly increase the cost of wages. Finally, from a structural perspective many firms are under the impression that both fields alone would not lead to a work load equivalent to a full time position.

Perspectivewise, different scenarios being thought of viable future usage for the curriculum. Stakeholders expressed interest in developing further courses on differen EQF levels, for which specific points would needed to be taken into account. Firstly, time and scope would need to be detailed out. Secondly, correspondingly to the EQF level, some specificities would need to be included, e.g. if a Master Course would be developed, probably some more focus on governance would be needed. Thirdly, providers should think about courses specifically designed for refreshing and updating knowledge and skills. To this end, selective courses can be developed.

Concerning the self-assessment, stakeholders welcomed the idea of having a tool for orientation at hand. In order to ensure the usability and user-attractiveness, it should be ensured that the extensive knowledge of information security and data protection will be covered to a reasonable extend, so that the test won’t become too complex and discourage potential users. The closely related validation of prior learning was finally also warmly welcome, as especially experienced professionals are difficult to find and most valuable to hire. Anything facilitating the recruiting process would lower the cost of entrance of new employees and facilitate SMEs to increase their information security.

9 Literature

Arbeitsmarktservice Österreich (2021): AMS Ausbildungskompass. Online verfügbar unter https://www.ausbildungskompass.at/, zuletzt geprüft am 30.07.2021.

Barlette, Yves; Fomin, Vladislav V. (2008): Exploring the Suitability of IS Security Management Standards for SMEs. In: *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)* 41, S. 308. DOI: 10.1109/HICSS.2008.167.

Bertelsmann Stiftung (2021): Über das Projekt - MYSKILLS - Berufliche Kompetenzen erkennen, zuletzt geprüft am 30.07.2021.

BKA (2021): BKA. Online verfügbar unter https://www.bka.de/DE/Home/home_node.html, zuletzt geprüft am 30.07.2021.

BMB (2017): Strategie zur Validierung nicht-formalen und informellen Lernens in Österreich. Online verfügbar unter https://www.qualifikationsregister.at/wp-content/uploads/2018/11/Strategie_zur_Validierung_nicht-formalen_und_informellen_Lernens.pdf, zuletzt geprüft am 30.07.2021.

BMBWF (2020a): Abschlüsse und Kenntnisse nachholen - Überblick zum Zweiten Bildungsweg. Online verfügbar unter https://erwachsenenbildung.at/bildungsinfo/zweiter_bildungsweg/ueberblick.php, zuletzt geprüft am 06.08.2021.

BMBWF (2020b): Schulen für Berufstätige. Online verfügbar unter https://www.bmbwf.gv.at/Themen/eb/zb/sfb.html, zuletzt geprüft am 06.08.2021.

BMBWF (2020c): Zweiter Bildungsweg / Abschlussorientierte Erwachsenenbildung. Online verfügbar unter https://www.bmbwf.gv.at/Themen/eb/zb.html, zuletzt aktualisiert am 06.08.2021, zuletzt geprüft am 06.08.2021.

BMDW (2021): Bundesrecht konsolidiert, Fassung vom 30.07.2021. Online verfügbar unter https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597, zuletzt geprüft am 30.07.2021.

Bowden, Amanda (2016): 2016_validate_AT. Online verfügbar unter https://cumulus.cedefop.europa.eu/files/vetelib/2016/2016_validate_AT.pdf, zuletzt geprüft am 30.07.2021.

BSI (2012): Leitfaden Informationssicherheit. IT Grundschutz kompakt (BSI-Bro12/311), S. 1–91. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile&v=3, zuletzt geprüft am 04.01.2019.

BSI (2016): Das IT-Sicherheitsgesetz. Kritische Infrastrukturen schützen. Hg. v. Bundesamt für Sicherheit in der Informationstechnik. Bonn (19). Online verfügbar

unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf?__blob=publicationFile&v=7, zuletzt geprüft am 13.01.2019.

BSI (2019): Gesetz zur Umsetzung der NIS-Richtlinie. Mehr Aufgaben und Befugnisse für das BSI. Hg. v. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter https://www.bsi.bund.de/DE/DasBSI/NIS-Richtlinie/NIS_Richtlinie_node.html, zuletzt geprüft am 13.01.2019.

Bundesnetzagentur (2015): IT-Sicherheitskatalog gemäß §11 Absatz 1a Energiewirtschaftsgesetz, S. 1–16. Online verfügbar unter https://www.dekra-certification.de/media/10-pdf-downloads/it-sicherheitskatalog-08-2015.pdf, zuletzt geprüft am 04.01.2019.

Bundesnetzagentur (2019): IT-Sicherheit im Energiesektor. Hg. v. Bundesnetzagentur. Online verfügbar unter https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheit.html, zuletzt geprüft am 04.01.2019.

Cedefop (2014): Spotlight on VET: Germany: Publications Office.

Datenschutz.org (2018): BDSG-neu: Neues Bundesdatenschutzgesetz | Datenschutz 2019. Hg. v. Datenschutz.org. Online verfügbar unter https://www.datenschutz.org/bdsg-neu/, zuletzt aktualisiert am 04.01.2019, zuletzt geprüft am 04.01.2019.

Della Istruzione, Ministero Pubblica (2007): Normativa AGOSTO 2007. Online verfügbar unter https://archivio.pubblica.istruzione.it/normativa/2007/dm139_07.shtml, zuletzt geprüft am 30.07.2021.

DIHK (2021): CHANCEN NUTZEN! Mit Teilqualifikationen Richtung Berufsabschluss. Online verfügbar unter https://teilqualifikation.dihk.de/, zuletzt geprüft am 06.08.2021.

Directive 1005/36/EC of the European Parliament and the Council on the recognition of professional qualifications (2005). In: *Official Journal of the European Union L 255*, S. 1–166.

Dorothea Fohrbeck (2012): Recognition of foreign professional qualifications - the Federal Government's new Recognition Act. BIBB. Online verfügbar unter https://www.bibb.de/en/23110.php, zuletzt geprüft am 29.07.2021.

DSB (2019). Online verfügbar unter https://www.dsb.gv.at/, zuletzt geprüft am 14.07.2021.

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 Union (2008): Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (Text with EEA relevance) - Publications Office of the EU. Online verfügbar unter https://op.europa.eu/en/publication-detail/-/publication/fdd70f57-7032-4121-92ae-ccf8ef68c15b/language-en, zuletzt geprüft am 30.07.2021.

European Union (2016): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). In: *Official Journal of the European Union L 119*, S. 1–88.

Eurostat (2020a): Database - Education and training. Online verfügbar unter https://ec.europa.eu/eurostat/web/education-and-training/data/database, zuletzt geprüft am 29.07.2021.

Eurostat (2020b): Number of tertiary education students by sex and level of education, 2018 (thousands). Online verfügbar unter https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Number_of_tertiary_education_students_by_sex_and_level_of_education,_2018_(thousands)_ET2020.png, zuletzt geprüft am 29.07.2021.

EURYDICE (2020): Poland - Validation of Non-formal and Informal Learning. Online verfügbar unter https://eacea.ec.europa.eu/national-policies/eurydice/content/validation-non-formal-and-informal-learning-53_en, zuletzt geprüft am 06.08.2021.

Gutwirth, Serge; Leenes, Ronald; Hert, Paul de (Hg.) (2015): Reforming European Data Protection Law. Dordrecht: Springer Netherlands (Law, Governance and Technology Series, 20).

IHK (2018): Überblick - Weiterbildungs-Informations-System (WIS). Hg. v. IHK. Online verfügbar unter https://wis.ihk.de/informationen/spezialthemen/it-weiterbildung/ueberblick.html, zuletzt geprüft am 12.01.2019.

Kersten, Heinrich; Reuter, Jürgen; Schröder, Klaus-Werner (2013): IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz. Der Weg zur Zertifizierung. 4., aktualisierte und erw. Aufl. Wiesbaden: Springer Vieweg (Edition <Kes>).

Landesbeauftragte für Datenschutz und Informationssicherheit Nordrhein-Westfalen (2019): Wann müssen Datenschutzbeauftragte bestellt werden? Hg. v. Landesbeauftragte für Datenschutz und Informationssicherheit Nordrhein-Westfalen. Online verfügbar unter https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzbeauftragte/Inhalt/Betriebliche_Datenschutzbeauftragte/Inhalt/FAQ/Bestellung_DSB.php, zuletzt geprüft am 12.01.2019.

Marcella (2003): Legislative Decree no. 196 of 30 June 2003: Data subject's right. Online verfügbar unter http://static.sif.it/SIF/resources/public/files/privacy/196-2003_EN.pdf, zuletzt geprüft am 30.07.2021.

OEAD (2021a): Aufgaben der OeAD | NQR-Koordinierungsstelle (NKS) - Qualifikationsregister. Online verfügbar unter https://www.qualifikationsregister.at/service/aufgaben-der-nqr-koordinierungsstelle-nks/, zuletzt geprüft am 30.07.2021.

OEAD (2021b): Das österreichische Bildungssystem. Online verfügbar unter https://www.bildungssystem.at/en/, zuletzt geprüft am 29.07.2021.

OEAD (2021c): Second Chance Education - Das österreichische Bildungssystem. Online verfügbar unter https://www.bildungssystem.at/en/second-chance-education, zuletzt geprüft am 29.07.2021.

OECD; Eurostat; UNESCO Institute for Statistics (2015): ISCED 2011 operational manual. Guidelines fro classifying national education programmes and related qualifications. Paris, France.

Pretto, Annamaria (2009): PROGETTO "RETE DI COMPETENZE. Online verfügbar unter http://www.piazzadellecompetenze.net/FSE/reteGarbin/GAR_1-3_ricerca_12-07-10.pdf, zuletzt geprüft am 30.07.2021.

Republic of Lithuania (2015): XI-242 Republic of Lithuania Law on Higher Education and Research. Online verfügbar unter https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/548a2a30ead611e59b76f36d7fa634f8, zuletzt geprüft am 30.07.2021.

Tritscher-Archan, Sabine (2020): leitlinien-nqr-sst-01-01-2020. Online verfügbar unter https://ibw.at/resources/files/2020/1/10/1991/leitlinien-nqr-sst-01-01-2020.pdf, zuletzt geprüft am 30.07.2021.

UNESCO Institute for Lifelong Learning (2017): Austria: Strategy for Lifelong Learning LLL:2020 issued in 2011 | UIL. Online verfügbar unter https://uil.unesco.org/document/austria-strategy-lifelong-learning-lll2020-issued-2011, zuletzt geprüft am 30.07.2021.

Valikom (2018): Procedure. Online verfügbar unter https://www.validierungsverfahren.de/inhalt/verfahren/ablauf, zuletzt geprüft am 29.07.2021.

Valikom (2021): ASSESS AND CERTIFY VOCATIONAL SKILLS. Online verfügbar unter https://www.validierungsverfahren.de/en/home, zuletzt geprüft am 30.07.2021.

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

Zintegrowany System Kwalifikacji (2020): What is the Integrated Qualifications System and how does it work? - Zintegrowany System Kwalifikacji. Online verfügbar unter https://kwalifikacje.edu.pl/what-is-the-integrated-qualifications-system-and-how-does-it-work/?lang=en, zuletzt aktualisiert am 06.08.2021, zuletzt geprüft am 06.08.2021.

National Adaption Plan

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/.