# Desk Research

## Summary Report from all countries

| Document Details: | |
|---|---|
| Reference | **TeBeISi** |
| IO / Activity | IO1 – Desk research |
| Author(s) | Dr. Paul Schober |
| Character | Summary Report from all partner countries (Austria, Germany, Italy, Lithuania, Poland) |
| Date | 15.02.2019 |

Funded by the Erasmus+ Programme of the European Union

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



.

Funded by the
Erasmus+ Programme
of the European Union

## Table of Content

## 1. Aim of the Summary Report

This report presents the main results of all National Reports, carried out in Austria, Germany, Italy, Lithuania and Poland. While the most important facts are summarized in this common report, you will find detailed information for each partner country in the respective National Report.

The IT sector is characterized by short innovation and product cycles among developers and manufacturers. The half-life of central elements of technical knowledge can be regarded as "short" here. Studies show that approx. 50% of the product- and performance-specific knowledge required by a technical employee in three years is not yet available today. This imposes high and dynamically changing requirements on IT employees and their qualifications. Learning and recognition of informal aspects (keyword "learning on the job") is becoming "the crucial factor in the IT sector".

The report focuses on the validation of learning outcomes from non-formal and informal learning in the field of Information Security and Data Protection and the job profiles of "Information Security" and “Data Protection” are addressed. In the participating countries, formal vocational qualifications exist for these purposes. Since in the entire occupational field, i.e. the labour market segment, many lateral entrants are active without degrees and work in a thoroughly solid manner in practice, the aim is to examine in a comparison of countries of the partners how non-formally and informally acquired learning outcomes can be determined diagnostically and validated on the basis of the examination regulations for formal degrees.

Against this background the aim of this report is to provide an overview of the offers from Vocational Education and Training System and the demands and needs of the labour markets in the field of Data Protection and Information Security and the related methods for validating informal learning in the partner countries.

In this regard, an overview of national rules and regulations concerning Information Security and Data Protection relevant for organisations in the profit and non-profit sector will be given.

The next step of the baseline research for TeBeISi is to carry out a field research to have an informed base to draft possible profiles for Information Security Officers and Data Protection Officers in two different competence levels (experienced staff & expert level).

**Definition of Terms**

As the terms Information Security and Data Protection are frequently slightly different used it will be clarified for this report here.

**Information security** Preservation of confidentiality, integrity and availability of information.

> Confidentiality Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
>
> Integrity Property of accuracy and completeness
>
> Availability Property of being accessible and usable upon demand by an authorized entity
>
> (Brookson et al. 2015, p.16)

**Data Protection**, also known as data privacy or information privacy, is the relationship between the collection and dissemination of data, technology, the public expectation of privacy, legal and political issues surrounding them.

> Privacy concerns exist wherever personally identifiable information or other sensitive information is collected, stored, used, and finally destroyed or deleted – in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. Legal framework within the EU is the General Data Protection Regulation (EU 2016/697) (Wikipedia 2019a).

## 2. Executive Summary of Main Outcomes in National Reports

### 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.

According to a KPMG study, 80% of Austrian companies run important processes with IT support. 63% speak of "highly confidential information," which will be stored in their computer systems. 56% of the companies are talking about a significant business interruption, if corporate data is no longer accessible. (KPMG 2013)

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 (DSG 2000), 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.

In relation of the recognition of non-formal and informal learning in the field of ICT, the National Qualifications Framework (NQF) is the basic tool to act as a transparency and translation instrument between the various qualifications and qualification levels of the individual educational sectors in Austria.

In principle, it is irrelevant in which educational institution a degree was obtained. The learning outcomes, which are certified by a qualification, are decisive for the placement. Depending on the concrete profile of a qualification, these learning outcomes can refer to a scientific discipline, a subject of study or to a concrete occupation or occupational field. It follows that very different qualifications may be at the same level without these qualifications being similar in terms of their concrete content.

Overall, the current annual "training performance" of the Austrian training system can be quantified with a total of almost 10,000 ICT training graduates in a narrower sense, although these data cover very different training levels. The largest share of all ICT graduates (about 40%), by educational path, is accounted for by vocational secondary schools. In second place are the universities of applied sciences, which account for around 20% of all ICT graduates. The proportion of women completing ICT training is currently around 26% and varies considerably depending on the training path. Due to demographic developments, however, a decline in the number of annual graduates can be expected by 2025, assuming constant IT rates. (IBW 2012)

In Austria, the following training paths are possible in the field of IT: "apprenticeship", "BMS" (vocational middle school,) "BHS" (vocational secondary school, e.g. commercial academy or higher technical college; incl. college and advanced training course), "FachHS" (university of applied sciences degree course), "Uni, HS" (university, university), "Unilehrgang" (university degree course) as well as further training offers at various adult education institutions or training institutes. (AMS 2016).

The ICT sector in Austria generates about 8.6 percent of total value creation. However, as generic technologies, ICT also impacts other sectors and enhances their productivity. An overall production value of EUR 36,6 billion including indirect effects can be assigned to the ICT sector. On balance, the ICT industry secures about 290,000 jobs in Austria.

The gap between job supply and demand in information technology (IT) is growing into a crater. According to the Austrian Federal Economic Chamber, at least 5000 IT positions cannot be filled in Austria in 2019.

## Germany

The corporate landscape in Germany is confronted with a large demand for IT security specialists at present and a further increase in demand in the near future. Due to the legal situation, information and data security in companies is of considerable importance and skilled workers are urgently needed. The main demand is for experts at operational and strategic level, usually in conjunction with a (presumed) university degree. These experts should not only have technical know-how, but also be familiar with the legal framework.

The requirements for IT security experts are therefore high. In addition to knowledge of the DSGVO (or BDSG-new) regulation, IT security experts need to know about the industry-specific legal situation of information security, especially if their company is active in the field of critical infrastructures.

The increasing demand for IT security experts on the part of companies is thus associated with a high requirement profile, which makes it more difficult to fill a new position than in hardly any other industry. Further education and training of employees therefore represent an important opportunity for companies to close this competence gap. On the employees' side, the possibility of validating their informal knowledge is gaining importance as they can communicate their skills more credibly.

The certification of knowledge and competences in the areas of information security and data protection is carried out by a large number of providers, but the learning content and the examination certificate are not standardised. That means there is a lack of clarity to the significance of a certificate outside the company for which it was acquired. However, it is possible to participate in a further training of the IHK to become an IT specialist by proving work experience, whereby a degree with DQR level 5 is obtained and participation in further certifications (DQR 6 and 7) is made possible. With regard to the validation of non-formally acquired competences, the IHK equates four years of work experience with a formally acquired qualification at EQR level 4, which gives professionals with informally acquired skills a good chance of entering the IHK's validated IT training programme.

In addition, the increased use of development centres offers an opportunity to determine the level of knowledge more precisely and, if necessary, to support the further training of IT specialists through targeted measures. The BSI also offers a certification procedure, which takes about 3 years. The competencies of the applicant are monitored during this time and if these competencies are maintained and expanded, a certificate is issued after the 3-year period. Other validation possibilities for informal competences are offered but are only partially checked by public authorities and therefore are only to a limited extent helpful for applicants.

In conclusion, it can be deduced from the current situation that most training pathways take place at DQR levels 5-7 and validation of DQR level 4 usually only includes admission requirements such as relevant work experience. There is therefore a gap for the validation of informally acquired competences at higher levels. In Germany, although there are possibilities for validating informal competences, it is questionable to what extent these are recognised as certifications by companies. There is a lack of an official recognition of informal competences, through which the skills of the applicants are presented in a manner acceptable to companies, so that suitable candidates can be selected for the respective job. In particular, the validation of very specific knowledge required for information security and data protection is still scarce.

Specific offers for SMEs regarding informally acquired competences cannot be found according to the current state of research.

## Italy

PA - Public Administration and businesses must network and be at the forefront of the battle for cyber security because 2019 promises nothing good on this front: attacks on the cloud to take over business data, new malware to hack smartphones, tablets and routers, identity theft via social networks.
Attacks using artificial intelligence will be used to collect and select as much information as possible, and a push will be made towards the ever-increasing creation of swarms of compromised servers, to be used to carry out complex attacks.

How can one try to defend oneself from all this? Following the expert tips, focusing more and more on the synergistic force of three fundamental aspects: culture-technology-organization.

Culture. It will be the main weapon to face the "traditional or low cost" attacks (phishing, crypto). It will be necessary to focus on actions of sensitization and knowledge of cybersecurity.

Technology. The focus will be on behavioural analysis of systems and artificial intelligence techniques to recognize and limit attack actions. It will be necessary to identify in the bud the condition of the attack and isolate it, in order to mitigate its "lateral movement".
Organization. Rules and policies will become fundamental in organizations to reduce misbehaviours, compartmentalizing "risk zones".

Thanks also to European directives and regulations, we are becoming aware that risks must be analysed and not only accepted, but above all mitigated by reasoning on appropriate safety measures.
For example, the European Union is already launching the idea of a competence centre in cybersecurity, while universities are increasingly starting to think of degree courses with specialisations in information security.
European regulations begin to generate the first sanctioning measures: the first sentences of the guarantors indicate how much the lack of basic concepts such as encryption, profiling and policies can weigh from the sanctioning point of view.
Moreover, from the point of view of awareness, it would be necessary to think of school programmes already in compulsory school on security issues, increasing television campaigns that are easily understood by all.

The PA and SME world will have to play an important role, trying to react by working on a common ground in the field of security.
It could be of great help to start an even stronger collaboration on this issue between the in-house of the territory and the trade associations and industrial unions that offer support services to their members (some examples in this direction have already been activated).
It will be necessary to develop better alerting services, establishing collaborations with the postal police forces, increasing the ability to info sharing, or communication and reporting of malicious events identified.
And always within the PA, the Regions can become points of aggregation and diffusion of the culture on security, with the strong help of experts.

In conclusion, the long battle over security and data protection is perhaps only just beginning and we will unfortunately still have to witness many more incidents, but it is important to react, to make cohesion and to grow by increasingly strengthening collaboration between the private and public modes.

## Lithuania

There is a transitional period in Lithuania for the introduction of information and data protection systems in enterprises. The legal framework is sufficiently developed in response to European Union directives. As this is a relatively new normative procedure, small and medium-sized enterprises, as revealed by the results of the study presented (discussed in section 4), face various difficulties in the practical implementation of legal norms, companies need to be more aware of the risks of personal data protection, to encourage and support business consulting with professionals, to promote and support the training of corporate employees on legal protection of personal data.

The analysis of job offers in the third to fourth quarters of 2018 revealed that job offers related to information security are more focused on IT professionals and related to data security - to focus more on legally trained staff.

In Lithuania, a network of training services on information and data protection for different levels of employees has been sufficiently developed. There is a certification system for information and data protection professionals. It should be noted that the training is mainly focused on large companies and personnel, IT and administration specialists of these companies. Meanwhile, NGOs and small businesses face a lack of access to such training, responding to the specifics of their organization, the cost of training, and so on.

## Poland

Information security is one of the most important and exciting career paths today all over the world. There is the need for an organization’s information security policy, this should not simply convey a plan of action, for example, its purpose, goals, applicability, importance and activities; most importantly organizations should also document who is ultimately responsible for carrying out the security agenda across the enterprise.

Development in technology as well as economic and social globalisation, have resulted in new challenges. As organizations become more dependent on technology, information in digital form have turn out to be more comprehensive and represent higher value of asset. Consequently, they have equally become priceless targets to skilled relentless cyber criminals. As more and more people engage in online banking and shopping; social networking, location-based services, cloud computing and mobile services; enormous volume of digital traces containing personal data are left all over the internet. If not well secured and controlled, personal information might become exposed to unauthorized individuals with malicious intents - ranging from spammers

and criminals to fraudsters and stalkers. Hence, the need to safeguard information resources, and protect personal data from malicious activities has become paramount to enterprise survival. As businesses struggle to keep up with the critical information security issues in the face of increasing risk of serious data beaches; data protection laws are changing in order to adjust to these risks.

The cyber security sector requires getting the right workers with the right skills to the right place at the right time. Cyber security is not just about technology. It is about people, and the range of technical and specialist skills that are needed to ensure that the services, systems and networks we use every day are secure.

Qualifications and competences in the sector IT – conclusions:

- Formal education institutions equip graduates with basic knowledge in the field of information technology;
- Non-formal education plays a key role in increasing the attractiveness of employment;
- Non-formal education is an element that adapts graduates of formal education to the needs of enterprises (it allows to acquire key professional skills);
- The role of education is crucial in the context of the need to update knowledge in IT;
- Narrow specializations result in the occurrence of professions that do not have developed professional qualification standards;
- Large diversity of companies and the requirement to know different applications results in different responsibilities and requirements even at the same positions;
- Multitasking causes the employment of people with qualifications / competences that go beyond the standard scope. The lack of knowledge related to the short life cycle of IT products imposes the necessity to acquire new competences;
- The lack of sharp boundaries between positions makes it difficult to identify specific qualifications and competences (penetration of the scope of requirements on different positions);
- The problem of identifying competences acquired in an informal way.

## 3. National Rules & Regulations concerning Information Security and Data Protection in SMEs & Nonprofit Organizations

## Austria

### *Information Security*

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. (BMEIA 2015)

The ISO/IEC 27001 standard, relevant to the information security management system (ISMS), describes information security as a "continuous improvement process" (CIP): (see BKA 2018)

Planning (Plan): Defining the ISMS, i.e. determining relevant security goals and strategies, creating an organization-specific information security policy and selecting specifically appropriate security measures.

Implementation (Do): Implementation and operation of the ISMS; i.e. implementing security measures, ensuring compliance and ensuring information security during ongoing operations, including in emergencies.

Check: Monitoring and checking the ISMS for its effectiveness; this means checking the existence, usefulness, compliance with security measures, but also gaining knowledge of incidents and common good practices.

Act: Maintenance and improvement of the ISMS; this means reacting to detected errors, weak points and changed environmental conditions and eliminating the causes of hazards. This requires renewed planning, which closes a continuous cycle.

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: (see BKA 2018)

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 (DSG 2000), 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 Labor 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, Leenes, de Hert 2015)

## Germany

### *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 (Bundesamt für Sicherheit in der Informationstechnik 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 (Bundesamt für Sicherheit in der Informationstechnik 2019b).

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 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). 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.

## Italy

As Italy is a member of the European Union, all national legislation relating to Information Security and Data Protection / Privacy derives from European Regulations and Directives.

In this sense, on May 16, 2018, the Council of Ministers approved the Legislative Decree to implement the NIS (Network and Information Security) Directive in our country.

The Italian government has opted for a "soft" approach, limiting itself for the most part to incorporating into the legislative decree what was already established by Directive NIS 2016/1148 on the security of networks and information systems.

This Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerns measures for a high common level of network and information system security in the European Union. In line with the requirements of Article 7 of the Directive, the transposing decree provides for the adoption of a national cybernetic security strategy by the President of the Council of Ministers.

The strategy should include, in particular, measures for the preparation, response and recovery of services following cyber incidents, the definition of a cyber risk assessment plan and cyber security training and awareness programs. Most of these elements are already addressed, for the most part, in the current national cybernetic security strategy, outlined in the National Strategic Framework for cybernetic space security of December 2013 and further developed by the National Plan for cybernetic protection and cybersecurity of March 2017. Both documents, in Italian, are attached to this report, as additional and complementary elements to what is reported below.

In summary, the two documents contain the following essential elements:

- The profiles and evolutionary trends of threats and vulnerability/risks of systems and networks, especially those of national interest;
- Tools and procedures to enhance cybernetic capabilities in Italy;
- The roles and tasks of public actors in the field of control;
- The strengthening of organizations and coordination methods at national level between public and private subjects;
- The promotion and diffusion of the culture of information security;
- The operation of the national structures and the connection with the various legislative interventions;
- The realization of protocols and standards of security;
- The development of awareness and communication actions;
- Finally, the implementation of a national "cyber risk management" system.

However, it will be necessary to update this strategy in order to ensure that all the elements referred to in Article 7 of the Directive are dealt with in a specific and detailed manner, in accordance with Community requirements. As regards the designation of the authorities responsible for implementing and supervising compliance with the NIS legislation, the institutional model chosen by the government is a "decentralized" one. In fact, as many as 5 national ministries (economic development, infrastructure and transport, economy, health and environment) are designated as "competent NIS authorities", each responsible for one or more sectors falling within its areas of competence.

Comparing the Italian legislation with other European realities, it can be affirmed that it is a model halfway between the strongly centralist French one, with a single competent authority, and the decentralized one of the Nordic countries, such as Sweden, where the regulatory and supervisory tasks in matters of cybersecurity are attributed to a series of public agencies competent for specific sectors.

The Security Information Department (DIS) is designated as the single point of contact under Article 8 of the Directive. The DIS will therefore be responsible for liaising with the European Union and coordinating with the cybersecurity authorities in the other Member States.

The current legislation also provides for the establishment within the Presidency of the Council of Ministers of a single "Computer Security Incident Response Team", called the Italian CSIRT, which will replace, merging them, the current National CERT (operating at the Ministry of Economic Development) and CERT-PA (operating at the Agency for Digital Italy).

This merger process could not be easy to manage, which could extend the time for the adoption of the Prime Minister's decree to be adopted later to regulate in detail the organization and operation of the CSIRT.

In any case, the Italian CSIRT will have technical tasks in the prevention and response to computer accidents carried out in cooperation with other European CSIRTs.

The implementing decree reiterates the general safety obligations provided for by the Directive in Article 14. In essence, operators of essential services must adopt technical and organizational measures "adequate" to manage risks and prevent computer accidents.

However, the decree specifies that when adopting such measures, operators must take due account of the guidelines that will be prepared by the Cooperation Group.

These guidelines are therefore of fundamental importance for demonstrating the adequacy of the measures adopted.

The competent NIS authorities may also require the adoption of specific security measures, in consultation with the operators of essential services.

It is therefore likely that operators will soon have more specific guidance on the security measures to be taken, in the form of guidelines or other administrative measures.

Similar security obligations are imposed on digital service providers, who will have to take technical/organizational measures to manage risks and reduce the impact of possible cyber incidents.

The elements to be taken into account by digital service providers for the management of cyber risks are better specified in Commission Implementing Regulation (EU) 2018/151 of 30 January 2018.

The implementing decree specifies that the processing of personal data in application of the decree is carried out in accordance with Legislative Decree no. 196/2003 (Privacy Code).

This reference has become (at least in part) obsolete with the final entry into force of the General Regulation on Data Protection (GDPR) on 25 May 2018, it is to the latter therefore that reference should be made.

## Lithuania

A new reading of the Law on Legal Protection of Personal Data of the Republic of Lithuania was adopted 16 July 2018. The purpose of this law is to protect the fundamental rights and freedoms of people, in particular the right to the protection of personal data, and to ensure a high level of protection of personal data.

Article 3 of the Law, points (2) and (3) state that it is forbidden to publicly disclose the personal code and to process the personal code for direct marketing purposes. Art. 5 defines peculiarities of personal data processing in work-related cases 1 p. 'It is forbidden to process data on convictions and criminal offenses of a candidate for employment or work, and personal data of a person, except where such personal data are necessary to verify that the person complies with the requirements for the performance of duties or work functions as defined in statutory and implementing legal acts"; 3 p. "When processing video and / or audio data in the workplace and in the premises of the controller of such data or in the areas where the controlled employees work, personal data relating to the monitoring of the behaviour, location or movement of employees shall be notified to such staff upon signature of informing of such processing or other means of proving the fact of informing. This law also defines the supervisory authorities, the provisions of these institutions on infringement proceedings, and the procedure for imposing administrative fines.

31 October 2018: Guidelines for Implementing Appropriate Organizational and Technical Data Security Measures for Personal Data Controllers and Managers were adopted; the document provides that the basic personal data security tool for the organization's personnel having access to personal data is clearly defined and documented responsibilities and roles, as well as competencies in dealing with personal data.

The organization shall have a register of IT resources used for the processing of personal data (hardware, software and network equipment). The register shall contain at least the following information: type of IT resources (e.g. server, workstation), location (physical or electronic). Managing the registry must be assigned to a specific person, such as an IT specialist. The document states that the organization must establish the basic procedures to be followed in the event of an incident or personal data breach, in order to ensure the continuity and availability of personal data processing in IT systems.

On 5 September 2018 the Recommendations for Small and Medium-Sized Enterprises on the Application of the General Data Protection Regulations were adopted. 27 April 2016 Regulations (EU) 2016/679 of the European Parliament and of the Council defined the protection of individuals with regard to the processing of personal data and on the personal data, how they can be processed, the length of time for which personal data must be collected, the duties of data controllers.

2 July 2018: a recommendation on procedures for identifying, investigating, reporting and documenting personal data breaches was adopted. Also in Lithuania there function and are in force other previously adopted legal acts and recommendations related to personal data protection: Recommendation on Records of Data Processing Activities, Related to the Protection of Personal Data: Recommendation on Records of Data Processing Activities (2018); Guidelines for Ensuring the Security of Personal Data Processed in Healthcare Facilities (2017); Recommendation On the Protection of Personal Data and Privacy in the Use of Wireless Networks (2017); Recommendation On Protection of Personal Data on Android Devices" (2015); Recommendation On the Use of Cookies and Similar Devices (2011) and other legal acts1

## Poland

There are many laws and ordinances in Polish legal regulations that should be known and used when creating an Information Security Policy. The implementation of security policy in the organization is caused by two aspects, the first is business and the other is legal. The policy created in organizations should comply with the law that is in force in Poland.

**The legal acts in Poland in which definitions, information and requirements for Information Security and Data Protection were included are:**

- The Act of 29 August 1997 on the protection of personal data (Journal of Laws 2002 No. 101 item 926, as amended) (Ustawa o ochronie danych osobowych);
- The Act of July 27, 2001 on the protection of databases (Journal of Laws of 2001 No. 128, item 1402, as amended) (Ustawa o ochronie baz danych);
- The Act of September 6, 2001 on access to public information (Journal of Laws 2001 No. 112, item 1198, from 2002 No. 153 item 1271, from 2004 No. 240 item 2407) (Ustawa o dostępie do informacji publicznej);
- The Act of 18 September 2001 with an electronic signature (Journal of Laws 2001 No. 130 item 1450) (Ustawa o podpisie elektronicznym);
- The Act of 18.07.2002 on providing electronic services (Journal of Laws of 2002 No. 144 item 1204) (Ustawa o świadczeniu usług drogą elektroniczną);

[1] https://www.ada.lt/go.php/lit/Valstybines-duomenu-apsaugos-inspekcijos-rekomendacijos/2

- The Act of July 16, 2004 Telecommunications law (Journal of Laws 2004 No. 171 item 1800) (Ustawa Prawo telekomunikacyjne);
- The Act of August 5, 2010 on the protection of classified information (Journal of Laws 2010 No. 182 item 1228) (Ustawa o ochronie informacji niejawnych);
- Act of 22 August 1997 on the protection of persons and property (Journal of Laws of 1997, No. 114, item 740) (Ustawa o ochronie osób i mienia);
- The Act of February 4, 1994 on copyright and related rights (Journal of Laws of 1994 No. 24, item 83) (Ustawa o prawie autorskim i prawach pokrewnych);
- Act of 24 May 2000 on the National Criminal Record (Journal of Laws of 2000 No. 50 item 580) (Ustawa o Krajowym Rejestrze Karnym);
- Act of July 5, 2002 on the protection of certain services provided electronically based on or consisting of conditional access (Journal of Laws of 2002 No. 126, item 1068) (Ustawa o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym);
- Act of February 17, 2005 on computerization of the activities of entities performing public tasks (Journal of Laws of 2005 No. 64, item 565) (Ustawa o infrormatyzacji działalności podmiotów realizujących zadania publiczne);
- Regulation of the President of the Council of Ministers of July 20, 2011 on the basic requirements for the security of telecommunications systems and networks (Journal of Laws 2011 No. 159, item 948) (Rozporządznie Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych);
- Regulation of the Minister of Finance of October 31, 2003 on detailed rules for creating, saving, storing and securing documents related to the conclusion and performance of insurance contracts (Journal of Laws 2003 No. 193, item 1889) (Rozporządzenie Ministra Finansów w sprawie szczegółowych zasad tworzenia, utrwalania, przechowywania i zabezpieczania dokumentów związanych z zawieraniem i wykonywaniem umów ubezpieczenia);
- Regulation of the Minister of Justice of April 28, 2004 on the method of technical preparation of systems and networks used to provide information for the collection of telephone call lists and other transfers of information and methods of securing IT data (Journal of Laws 2004 No. 100 item 1023) (Rozporządzenie Ministra Sprawiedliwości w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczania danych informatycznych);
- Regulation of the Minister of Interior and Administration of 29 April 2004 on the documentation of the processing of personal data and technical and organizational conditions which should be met by devices and IT systems used to process personal data (Dz.U.2004 No. 100 item 1024) (Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych);
- Regulation of the Council of Ministers of July 20, 2011 on determining technical and organizational conditions for qualified entities providing certification services, certification policies for qualified certificates issued by these entities and technical conditions for secure devices used for submission and verification of electronic signature (Journal of Laws of 2002 No. 128 item 1094) (Rozporządzenie Rady Ministrów w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego);

- Regulation of the Council of Ministers of May 29, 2012 on physical security measures used to secure classified information (Journal of Laws of 2012, No. 115, item 683) (Rozporządzenie Rady Ministrów w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych);
- Regulation No. 57 of the Minister of National Defense of December 16, 2011 on a special way of organization and operation of secret offices and other than the secret registry of organizational units responsible for processing classified information, the manner and mode of processing classified information, and the selection and application of physical security measures (Official Journal of the Minister of National Defense No. 24 of 30 December 2011) (Zarządzenie Ministra Obrony Narodowej w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie informacji niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego).

Until the EU General Data Protection Regulation ('GDPR') takes effect in May 25th, 2018, the primary data protection legislation in Poland was the Personal Data Protection Act of 1997 (Ustawa o ochronie danych osobowych). The General Data Protection Regulation 2016/679 (GDPR), in Polish *Rozporządzenie o ochronie danych osobowych* (*RODO*), of the European Parliament and of the Council of 27 April 2016, repealing Directive 95/46/EC [95/46/WE][2], entered into force in Poland on 25 May 2018. The purpose of this normative act is to harmonise the protection of fundamental rights and freedoms of natural persons with regard to the processing of their personal data, while at the same time ensuring the safe free flow of such data between Member States.

Privacy law has its roots in the Constitution of the Republic of Poland of 2 April 1997[3], and in particular in Article 47, which guarantees the right of every citizen to a private life. This constitutional principle was further specified in Articles 23 and 24 of the Act of 13 April 1964 of the Civil Code[4], which protect the personal interests of natural persons.

Data protection and information security are also guaranteed by many sector-specific regulations. There are key legal acts covering data protection in the areas of banking law, insurance law, telecommunications, e-commerce, pharmaceuticals and health law, and other areas where sector-specific provisions regulating how data should be processed are present.

[2] Regulation (EU) 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 [95/46/WE] (The Official Journal of the European Union L.2016.119.1).
[3] *Journal of Laws No. 78, item 483.*
[4] *Journal of Laws 2014, Item 121 with amendments.*

## 4. Vocational and Continuing Education and Training in this area

### Austria

Overall, the current annual "training performance" of the Austrian training system can be quantified with a total of almost 10,000 ICT training graduates in a narrower sense, although these data cover very different training levels. The largest share of all ICT graduates (about 40%), by educational path, is accounted for by vocational secondary schools. In second place are the universities of applied sciences, which account for around 20% of all ICT graduates. The proportion of women completing ICT training is currently around 26% and varies considerably depending on the training path. Due to demographic developments, however, a decline in the number of annual graduates can be expected by 2025, assuming constant IT rates. (IBW 2012)

Particularly in ICT occupations, parts of the specialist knowledge have a very short validity, which means that continuous further training is of central importance, but there is also a very wide range of access options.

In Austria, the following training paths are possible in the field of IT: "apprenticeship", "BMS" (vocational middle school,) "BHS" (vocational secondary school, e.g. commercial academy or higher technical college; incl. college and advanced training course), "FachHS" (university of applied sciences degree course), "Uni, HS" (university, university), "Unilehrgang" (university degree course) as well as further training offers at various adult education institutions or training institutes. (AMS 2016).

### Germany

There are various Master's programs in the fields of information security and data protection. The profile area of cyber security at Darmstadt Technical University, which offers the Master of Science (M.Sc.) in IT security, deserves special mention here.

Within the framework of vocational training, the IHK offers seminars, trainings and apprenticeships in several areas. Seminars take place on data protection in the personnel area and data protection officers in the company, the "White Hacker" is offered as a training. Apprenticeships with state-approved DQR level 4 are possible to become an information technology clerk, an IT system clerk and an IT system electronics technician (IHK 2018b, 2018c).

Building on this, further training to operative (DQR level 6) and strategic (DQR level 7) professionals is possible (see Figure 3): a specialist qualification (DQR level 5) in one of 14 possible fields of work, relevant for this is the IT security coordinator, allows admission to the examination of an operative as well as a continuing strategic professional. In the field of continuing vocational training, the specialist qualification forms the link between the vocational training and the level of the operative professionals regulated in the continuing vocational training. Figure 3 illustrates the continuing training structure of the IHK.

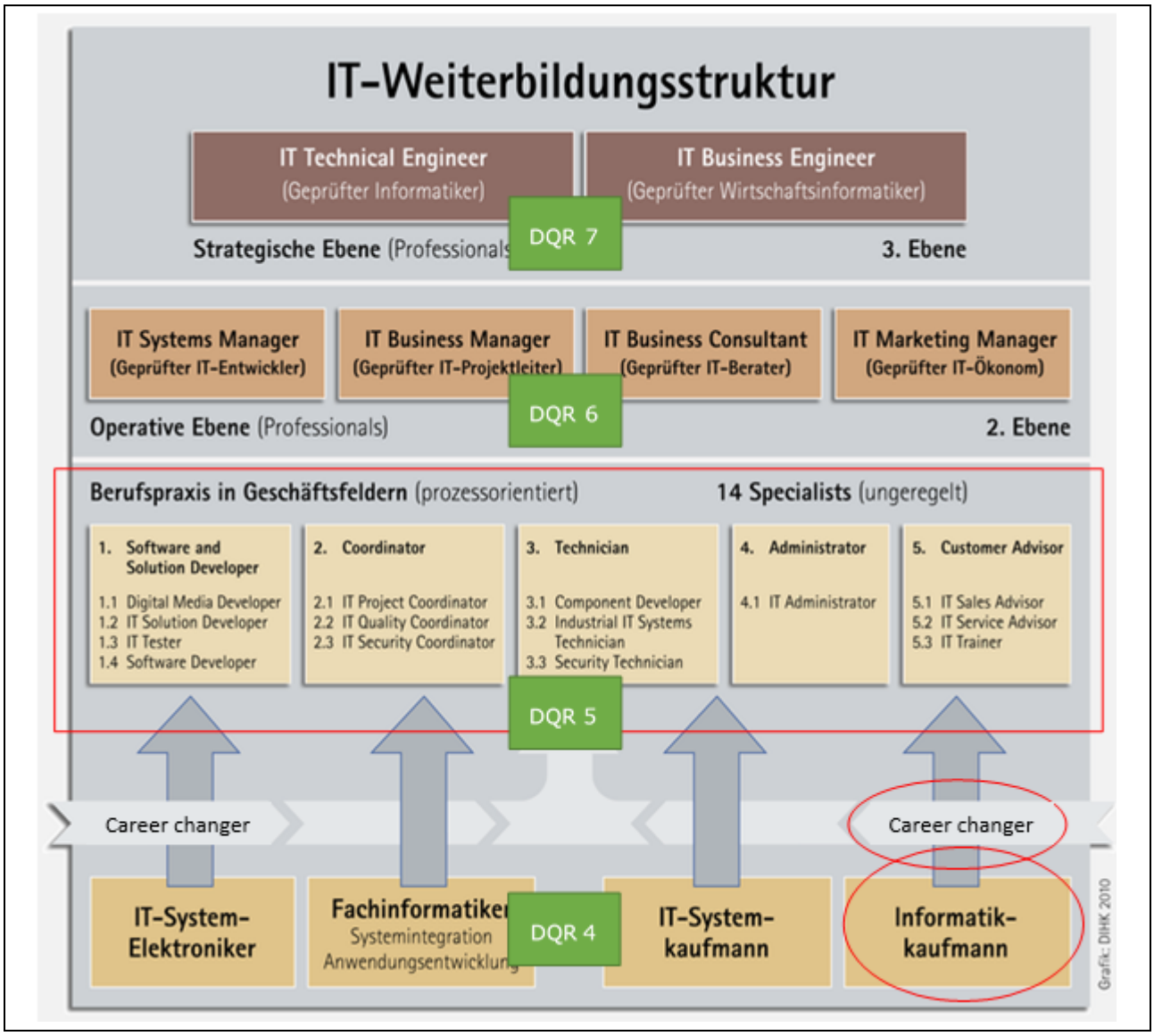


*Figure* **1***: Continuing training structure of the IHK*
*Source: based on IHK (2018d)*

A completed vocational training to participate in a further training to become an IT specialist is, however, not absolutely necessary, as can be seen from the figure above.

Admission requirements exist above all in the area of continuing education under public law, e.g. for the state-recognized examination for IT professionals. For the certificate area of continuing education, such as that of an IT specialist, there are usually no requirements. Nevertheless, admission requirements determine the qualification for entering a certain level of continuing education. The qualification to become an IT specialist also requires a certain entry level. In connection with the certification of individuals, it was stipulated that a continuous training participant must either

- a vocational qualification in an IT profession or
- other professional qualifications and at least one year's relevant professional experience in the IT field, or
- must have at least four years' relevant professional experience.

Those who, by presenting certificates or by other means, can demonstrate that they have achieved the qualification justifying admission to certification are also admitted. In order to ensure the entry level of their qualification offers for IT specialists, the IHKs comply with these admission requirements.

In order to improve the competence-related self-assessment of people who want to validate non-formal competences, so-called Development Centers (DC) are used. They represent a special form or further development of the Assessment Centre (SC). These are procedures in which the participants go through different diagnostic modules (e.g. interviews, role plays, psychological test procedures, etc.) for two to three days and receive detailed feedback on their results (Klebl und Nerdinger 2010). The IHK offers three to four-day DC for business founders (IHK 2018a).

However, the use of DCs in the area of IT security is not known.

## Italy

On 25 May 2018, the General Data Protection Regulation (GDPR) was definitively applied throughout Europe (after a two-year transition). As is well known, it is the normative instrument wanted by the European Commission, to protect more the privacy of the EU citizens, strengthening and rendering more homogeneous the protection of the personal data.
It is an event that has seen many companies (especially smaller ones) in difficulty and will affect a lot of investment and efforts of Italian companies, but it is also an extraordinary opportunity to raise awareness and implement a series of specific measures and interventions, especially in training.
In this sense, from the end of 2017 until today, tens of thousands of training initiatives at national level have been offered by public and private entities and have addressed the issues dealt with in this report with different levels of detail (for example: from simple workshops for initial basic information, to paths, such as master, much more detailed and for specialist figures).
These regulatory obligations have also pushed the IT security market: in 2017, total investments (mainly technical adjustments and training) exceeded one billion euros in Italy! (*source: Information Security & Privacy Observatory of the School of Management of the Politecnico di Milano*)
In any case, the research shows, SMEs are not so lacking on the subject, at least in the area of cybersecurity. The level of adoption of solutions dedicated to information security increases as the size of the company increases, reaching 93% in medium-sized enterprises.

Remaining precisely on the latter, about half (44%) have technological solutions considered sophisticated, such as intrusion detection systems or identity and access management. In small businesses, basic tools such as antivirus and antispam are particularly widespread, while micro-businesses are particularly unprotected: 30% of them do not, in fact, adopt any type of solution.

Remaining on the main reasons for spending by SMEs, there is a strong demand for customer data protection (45% of the sample made up of 947 micro, small and medium businesses), followed by compliance with regulations (19%) and the need to defend oneself after having suffered cyber-attacks (11%).

As mentioned, as the company's reality increases, so do investments and information security solutions. The prevalent share (78%) of specific expenditure is held by the large companies.

By removing the share dedicated to adapting to GDPR, expenditure is still mainly oriented towards traditional security components, such as business continuity & disaster recovery (19%), network security (14%) and security testing (9%).

## Lithuania

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"[5] that ai mis 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 organization's IT infrastructure. UAB "Atea "[6] 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 [7] 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"[8], 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 nonprofessionals". 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

## Poland

Security experts agree that people are the critical factor in protection of organisations' cyber assets. The end-users access the assets on a regular basis and in most cases either they lack the security knowledge necessary to protect them or they know how to avoid protection mechanisms – in both cases the result is the same, namely the exposure of the cyber assets to threats.

At the same time the majority of organisations concentrate their information security budget on technical solutions. This is because technical methods are well-defined and comprehensible and give an illusion that when applied all security issues will be solved. This approach tends however to be ineffective. Surveys show that despite the gradually increasing investments in technical controls the number of intrusions reported annually also continues to rise. Interestingly, there are reports claiming that the majority of breaches were caused by insiders.

[5] www.cybersecurityacademy.lt
[6] www.atea.lt
[7] www.nrdcs.lt
[8] www.kompetenc.lt

Technical solutions cannot make a network more secure than activities of people who use it, because poor user practices overcome the even the most carefully planned security system.

Educating and raising security awareness among personnel is like expanding the information security department into the whole organisation.

Data protection officers and experts are in high demand in both the public and private sectors. Several higher-education bodies offer postgraduate studies focused on Security information and Data Protection. In Poland there are a lot of trainings in the field of Information Security and Data Protection.

## Existing Training Offers in the field of Information Security and Data Protection

In the respective National Reports from Austria, Germany, Italiy, Lithuania and Poland you find tables of selected training offers in this fields, categorized by the following criteria:

- Name of Training Course
- Main Content / Objective
- Target Groups (basic /intermediate / proficiant user)
- Skills acquired (professional, social and transversal)
- Kind of Testimonial

## 5. Jobs offered in the field of Information Security and Data Protection

### Austria

The ICT sector in Austria generates about 8.6 percent of total value creation. However, as generic technologies, ICT also impacts other sectors and enhances their productivity. An overall production value of EUR 36,6 billion including indirect effects can be assigned to the ICT sector. On balance, the ICT industry secures about 290,000 jobs in Austria.

The gap between job supply and demand in information technology (IT) is growing into a crater. According to the Austrian Federal Economic Chamber, at least 5000 IT positions cannot be filled in Austria in 2019.

However, the growth in demand of ICT sector is strongly industry-specific: in the Internet of Things (IoT) segment, the demand for IT security experts increased by 370% compared to 2016. In cloud computing, demand increased by 138%, followed by application security (33%), mobile applications (29.9%) and compliance (22.4%)

Overall, the demand for IT security experts across all industries increased from 12% of all companies in 2015 to 20% in 2017. 28% of all companies are looking for software developers for security (compared to 17% in 2015) (Berg 2017).

### Germany

According to BITCOM, there were 55,000 vacancies for IT specialists at the end of 2017, an increase of 20% compared to the previous year in Germany. This increase is most noticeable in the area of IT security experts: there is a particularly strong imbalance between the jobs offered and the number of applicants. For example, there were about four advertised positions for one security engineer, the same ratio prevailed for IT consultants with IT security expertise. In the case of IT administrators, there were still 3 advertised positions for every applicant. The most difficult field to fill in IT security in German companies is network security, followed by mobile applications and risk management (Berg 2017).

However, the growth in demand is strongly industry-specific: in the Internet of Things (IoT) segment, the demand for IT security experts increased by 370% compared to 2016. In cloud computing, demand increased by 138%, followed by application security (33%), mobile applications (29.9%) and compliance (22.4%) (Berg 2017).

Overall, the demand for IT security experts across all industries increased from 12% of all companies in 2015 to 20% in 2017. 28% of all companies are looking for software developers for security (compared to 17% in 2015) (Berg 2017).

The increased demand for security experts is also reflected in the average salaries, which at €75,000 are higher for employees without personnel responsibility than for project managers or SAP consultants (Mesmer 2018).

An evaluation of job offers in the IT security sector has shown that around 60% of job offers are directed at IT security, data protection and data security specialists. Furthermore, approx. 30% of the job offers were directed at IT consultants and approx. 6% at software developers specializing in IT security. The task most frequently described was "developing, implementing and monitoring concepts, guidelines and strategies" (68.7%). More than half of the ads examined required work experience. With regard to concrete specialist knowledge, experience in system or network administration was required in 26.2% of the advertisements and knowledge of the ISO/IEC 27000 series of standards was explicitly required in around a quarter of all advertisements.

With regard to the required certification, a degree in computer science (70%) or business informatics (31.9%) was required by a large margin. However, candidates with IT or computer science training also had good chances (26.8%). A completely new development can be seen in the required qualification of a law degree with 16.3% (Blindert 2018).

With these facts in mind, most positions are advertised in the areas of Consultant Information Security, Data Protection Officer, Programmer, IT-Consultant, Advisory and Compliance as well as Legal Affairs.

In order to address the security concerns of companies, the job of Chief Security Information Officer (CISO) has existed for some time now. He is responsible for information security in the company (Whitten 2008, S. 15). A combined search with the keywords "CISO" and "job" in common job portals and the subsequent screening of the job offers revealed that the companies expect a completed degree or a comparable education with several years of professional experience, various certificates such as ISO 27001 or CISM as well as expert knowledge in information security management. An input at the job portal "Indeed" of the search term "CISO" delivered 64 hits, while an input of the term "data security" yielded approx. 12,000 hits and "information security" approx. 1,200 hits.

## Italy

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 analyzed: 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 analyses 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.

## Lithuania

According to the data of 7 January 2019, there were 297 proposals for IT specialists on the website CV.lt. However, the ads did not specifically distinguish that.

11-26 July 2016 public opinion and market research company „Spinter Tyrimai" on behalf of the Human Rights Monitoring Institute, conducted a survey of business entities operating in Lithuania on data protection in Lithuania. The survey was carried out throughout Lithuania and was attended by representatives of 50 companies operating in Lithuania. Respondents were selected using the quota selection method, applying business type quota: startups - telecommunication and financial companies – and others, respectively 60 - 20 - 20. It appeared that businesses surveyed believe that the current legal regulation of data protection in Lithuania is sufficient.

Most believe that the legal regulation of Lithuania is sufficient, there are telecommunication and financial services companies (80%), the least - among other companies (60%). At present, telecom and financial services companies are among the most supervised, so they can best express their attitude towards the existing regulatory regime as well. Almost half of the respondents (48%) did not have the opinion whether the penalties provided for in Lithuanian legislation for violations of data protection requirements were sufficient at the moment. The other half (46 percent) believed that the punishment was sufficient, and the minority consider the punishment insufficient.

As mentioned above, penalties for violations of data protection requirements in Lithuania were among the lowest in the EU, but they were applied relatively frequently and for minor violations (e.g. non-registration as a data controller - an obligation that is generally repealed by the General Data Protection Regulation). Most of those who did not know about punishment were among other companies (70%), and most of those who thought that punishment was sufficient - among startups (53.3%). 55.6 percent companies that did not register as personal data controllers did not have an opinion or did not know about penalties for violations of data protection requirements, the number of such respondents among registered companies was 28.6%.

These results could be explained by the fact that registering as a personal data controller is one of the main administrative and bureaucratic duties of personal data controllers in accordance with the Law on Legal Protection of Personal Data of the Republic of Lithuania. Compulsory instructions and sanctions of the State Data Protection Inspectorate (further SDA) are often imposed for non-compliance.

As a result, companies that have registered as personal data controllers are more likely to face possible sanctions for violations of legal protection of personal data. The encouraging result is that the majority (74%) of the survey participants trust the institutions responsible for the supervision of privacy and personal data protection in Lithuania: 12%. fully trusted, 62 percent are more likely to trust. Most companies trusting Lithuanian institutions are among telecom and financial services companies: even 80 percent. replied that they are more likely to trust the Lithuanian authorities; however, there was no single response amongst them that they had full confidence in the institutions.

Most of the companies surveyed (even 72 percent) currently attach great importance to data protection. Most often, companies solve personal data protection problems with internal resources: the majority of respondents say that these problems are solved by a staff / administration employee (86%), 44%. - IT employee, 40% has a dedicated employee who takes care of data protection. Very few companies apply for assistance to external specialists - data protection specialists (6%), IT service providers (4%) or lawyers (2%).

In all telecom and financial services companies (100%), data protection issues are solved by personnel / administration staff as well as by 50%. these companies have a dedicated employee and 40 percent these problems are solved by IT staff. These companies do not seek help from outside specialists.

The situation among startups and other companies is similar, only among these companies there are several respondents who apply for help from external specialists. One company said that it is not solving data protection issues, and no such companies have emerged among startups and telecom and financial services companies.

Most respondents (74 percent) do not implement data protection for employee training (or do not allot any budget for that). From 26 % conducting training - 22% conduct trainings at least once a year, 4 % conduct trainings less than once a year. Data protection training is not carried out by 80 % of startup and telecom and financial services companies and 50 % of other companies. Among registered personal data controllers' enterprises there is higher percentage (78.6%) of non-training respondents than among non-registered companies (72.2%).

These results are worrying as they show that companies are not fully aware of the dangers to personal data in the cyberspace. Companies rely too much on internal resources, do not consult specialists and do not invest in training. In addition, companies that have registered as personal data controllers consider that they have fulfilled their formal obligations to protect personal data. According to the results of the survey, companies need to be more informed about the risks of personal data protection, to encourage and support the consultation of companies with specialists, to promote and support the training of corporate employees on the subject of personal data protection.

The research revealed the tendencies of legal protection of personal data in Lithuania. To sum up, the protection of personal data is not a novelty for Lithuanian business. Companies understand the importance of data protection and attach great importance to it

## Job offers in the field of Information Security and Data Protection

In the respective National Reports from Austria, Germany, Italiy, Lithuania and Poland you find tables of selected training offers in this fields, categorized by the following criteria:

- Job offer / enterprise
- General description
- Skills required (professional, social and transversal)
- Weblink

## 6. Existing Methods for Assessing and Certification of Vocational Skills acquired outside formal Education

### Austria

Recognition of prior learning and the Validation of non-formal and informal learning does not have a very long tradition in Austria.

The vision of the National Lifelong Learning Strategy to consider non-formal and informal education processes as equal to formal education is confronted with the Austrian reality: In the higher education system, the recognition of achievements is limited to those competences that can be proven through formal certificates. Access to higher education is typically and especially gained through the general university entrance qualification. Previous achievements are recognised by proof of certificates acquired in the formal education system. (AQA 2016)

This circumstance reflects in essence the Austrian legal framework. Against the backdrop of international developments and the increasing importance of lifelong learning it is necessary, though, to make society realise the added value of recognising experiences which were gained outside the formal education system and to promote permeability between non-academic and higher education.

Therefore, the main driving force in this field are the implementation of the European Qualification framework in Austria and the work done by Cedefop (European Centre for the Development of Vocational training).

Validation is, first, about making visible the diverse and rich learning of individuals. This learning frequently takes place outside formal education and training – at home, in the workplace or through leisure time-activities – and is frequently overlooked and ignored. Validation is, second, about attributing value to the learning of individuals, irrespective of the context in which this learning took place. Going through validation helps a learner to 'exchange' the outcomes non-formal and informal learning for future learning or employment opportunities. The process must generate trust, notably by demonstrating that requirements of reliability, validity and quality assurance have been met. These elements of visibility and value will always have to be taken into account when designing validation arrangements, although in different ways and combinations.

The above definition does not limit validation to a particular institutional context. While it is most commonly found within education and training, making it possible for individuals to acquire a formal qualification on the basis of non-formal and informal learning, validation is also carried out by several institutions and stakeholders outside education and training: labour market authorities, economic sectors, enterprises and voluntary organisations. The multiple outcomes of validation, ranging from formal qualifications to enterprise internal proofs of acquired competences, are all united through their efforts to increase the visibility and value of the learning taking place outside classrooms. To clarify the basic features of validation, the recommendation identifies four distinct phases: identification; documentation; assessment; and certification. (Cedefop 2015)

These phases are mixed and balanced in different ways, reflecting the particular purpose of each validation arrangement. When working towards a formal qualification, the robustness and credibility of the assessment stage are crucial. In other cases, for example in relation to voluntary work, more emphasis is given to identification and documentation, less to formal assessment and certification. However, the four phases are likely to be present in all validation arrangements. The purpose of validation is to produce proof of learning, potentially to be exchanged into future learning and/or work. This requires identification, documentation and assessment of the learning in question to refer to an agreed and transparent reference point or standard. In validation for formal qualifications, official standards used by the education and training system/institution will largely define the requirements of the validation process.

In other settings, as when mapping competences in enterprises, internal and less formal reference points will be used. While the same elements of identification, documentation, assessment and certification will be found in both cases, their relative 'weighting' differs significantly. Overall, the extent to which validation process outcomes can be transferred and exchanged very much depends on the extent to which the resulting document, portfolio, certificate or qualification is trusted by external parties and stakeholders, which reflects the way the four phases have been designed and carried out. Validation arrangements need to be presented in a way that clarifies their main purpose and allows individuals to choose the form best suited to their particular needs. A person not interested in acquiring a formal qualification should be able to opt for a solution giving more emphasis to identification and documentation phases. Since validation has been found to influence positively individuals' self-awareness and self-esteem, it should be about individual choice: arrangements must be designed to allow the individual to opt for the most cost-efficient solutions, possibly for limited documentation rather than full, formal certification.

There are several validation arrangements closely connected with the labour market, but only a few of these validation procedures have a legal basis and therefore result in formal qualification. In other words, many of them aim at obtaining non-formal qualification. Here we again have some examples for you (see: https://vince.eucen.eu):

- The Austrian Public Employment Service Vienna offers "competence checks" for asylum seekers. These checks include the validation informal learning (outside school or university, e.g. work experience).
- In some federal states there are institutions which validate prior learning. For example, in Burgenland, the Volkshochschule (VHS) is certified to validate prior learning.
- When it comes to recognition of formal vocational education, the platform www.berufsanerkennung.at gives guidance and shows success-stories of people, who went through validation procedures.
- If a validation candidate has a foreign formal vocational qualification but lost the documents, following contact point gives advice: http://www.berufsanerkennung.at/en/advice/

First pilot projects in the third sector were conducted in 2012. Back then, the project team examined how acquired skills in volunteering (volunteer firefighters and emergency medical services) could be integrated within a future national qualifications' framework. Now, as the Austrian Qualifications Framework has been installed, non-formal learning in the volunteer sector is matched to qualifications levels. The process started in March 2016 and is ongoing.

## Germany

Due to its complexity, a data protection officer is legally obliged to undergo training. Pursuant to art. 39 paragraph 2 DS-GVO, the company employing the data protection officer has the duty to support him in the performance of his tasks and, in particular, to provide him with the resources required to perform his duties and maintain his expertise. Therefore, it must also facilitate appropriate qualification. The „Society for data protection and data security e.V." (Gesellschaft für Datenschutz und Datensicherheit e.V.) has been offering training concepts for the training and further education of data protection and security officers in companies for 30 years (GDD 2018).

The BSI offers several certification methods for information security. The ISO 27001 is a certificate for companies that is issued only after an external audit and certifies that the company has basic IT protection (Bundesamt für Sicherheit in der Informationstechnik 2018c). It is not a certification for a person regarding their competences, but is intended exclusively for companies.

The entire certification procedure of the BSI for persons is shown in Figure 4 and takes about three years. After a positive examination of the application, the applicant is evaluated.

The competence assessment is carried out by an external service provider. If the applicant passes this evaluation phase, his competences are monitored and maintained for three years. After completion of the certification phase, the applicant submits a new application and receives a certificate if the evaluation is positive. The certification is limited to a period of three years (Bundesamt für Sicherheit in der Informationstechnik 2017, 2018a).

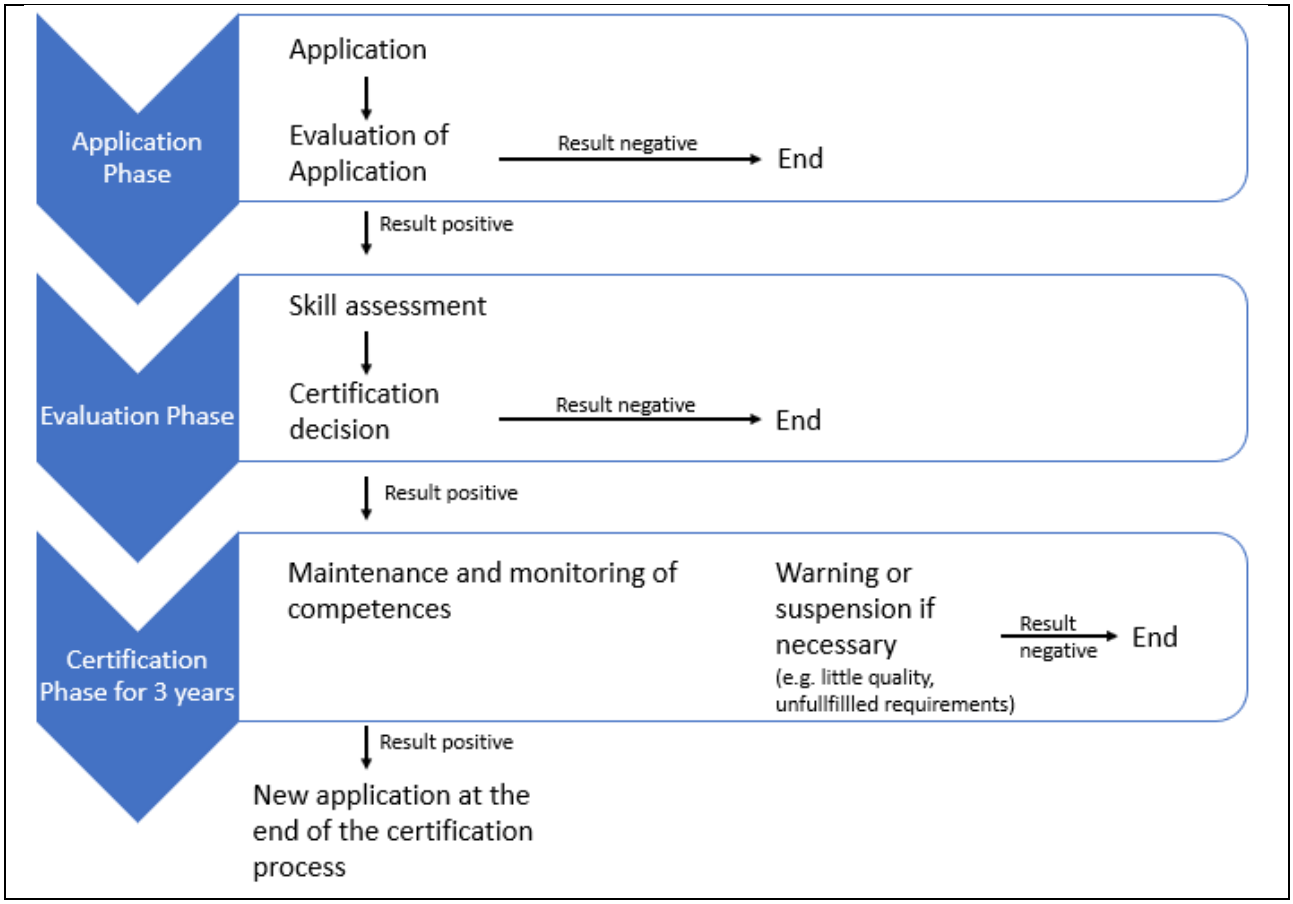


*Figure 2: Certification procedure of the BSI*
*based on Bundesamt für Sicherheit in der Informatinstechnik 2017, p. 6*

Certification is possible as a: Audit team leaders, De-Mail auditor, Smart Meter Gateway administrator auditor, "Secure E-Mail Transport" auditor, RESISCAN auditor for BSI-TR 03138, Secure CA Operation auditor, IS auditor, penetration tester, CC evaluator & Common Criteria training, TR auditor, BOS interoperability tester/ZPL employee.

Other providers such as the Academy of the DGI (German Society of information security AG - Deutsche Gesellschaft für Informationssicherheit AG), EDV-Fortress or TÜV offer training courses on basic IT protection, which, however, are not checked for content or quality by the BSI, as already mentioned in Chapter 3 (Bundesamt für Sicherheit in der Informationstechnik 2019a; BayLDA 2016). A complete overview is provided in Table 7 (see Annex).

Valikom offers a validation procedure in cooperation with the IHK and the Chamber of Trade (Handwerkskammer - HWK) (https://www.validierungsverfahren.de/startseite/). The target group here are people who:

- are at least 25 years old
- regardless of their current employment status
- have acquired professional skills at home or abroad
- but cannot prove this by means of a degree
- can prove relevant professional experience.

The validation process is divided into the following steps:

1. The applicant must report to a contact person (at HK or IHK).
2. An advisory interview follows with this contact person, discussing the validation process and the choice of the appropriate reference occupation. The reference occupation corresponds to a professional qualification.
3. The relevant skills of the applicant are described, and a curriculum vitae is drawn up which reflects the skills (everyday working life, training and further education, everyday life if relevant). These competences are entered in a self-assessment form.
4. The applicant's competences are compared with those required for the reference occupation.
5. The application documents for the validation are submitted to the chamber, which evaluates in which activities of the reference occupation an external evaluation will take place.
6. The external evaluation is carried out by experts of the respective reference occupation and tests the applicant's abilities in practice. This includes work samples, a technical discussion or trial work in a company.
7. The expert submits the results of the external evaluation to the chamber.
8. Depending on the result of the external evaluation, the chamber shall issue a validation certificate confirming full or partial equivalence with the reference occupation.

Another validation of professional competences is offered through the website https://www.myskills.de/. In cooperation with the Employment Agency, applicants carry out a computer-based test on the basis of which a certificate is issued. The test is so far only for eight occupational groups available, which limits it very much. Valikom on the other hand is by far more detailed and contains a practice test, which makes it more valuable for applicants and enterprises.

The DQR working group (the coordination group responsible for the development of the DQR set up by the Federal Ministry of Education and Research and the Conference of the Ministers of Education and Cultural Affairs of Germany) has not yet published its own validation methods for non-formally and informally acquired competences, which is why allocations to existing DQR levels are not yet possible.

## Italy

At the end of 2017, the Data Protection Supervisor has once again commented on the subject of the Data Protection Officer.

In practice, it does not matter whether the DPO has certifications, the DPO must be trained and have specific and multidisciplinary skills, but there is no evidence that it has a certification (of whatever nature it is and whatever value it has).

In the Guarantor's opinion, public administrations, as well as private subjects, will have to choose the Personal Data Protection Officer with particular attention, verifying the presence of specific skills and experiences.
In practice, therefore, no formal attestations are required on the possession of knowledge or registration in appropriate professional registers: it is only necessary, however, that the DPO can ensure the correct and complete execution of its tasks.

Of particular importance is the specification of the Guarantor for which the DPO must have a thorough knowledge of the rules and practices on privacy, as well as the rules and administrative procedures that characterize the specific area of reference.

Obviously, this could lead to "sectoral" DPOs considering the fundamental differences that exist between different market sectors.
Furthermore, the Guarantor recommends that in the selection process, priority be given to subjects who can demonstrate professional qualities appropriate to the complexity of the task to be performed, perhaps documenting the experience gained, participation in master's degrees and study/professional courses (in particular if the level reached is documented).
In the end, therefore, the attestations of professional competence achieved, or training carried out can be useful for evaluating a candidate but do not represent and do not amount to a "qualification" for the performance of the role of the DPO.

Moreover, the current legislation and European Regulation No. 679/2016 **do not provide** for the establishment of a register of "Data Protection Officers" that can certify the requirements and characteristics of knowledge, skills and competence of those who are registered.
Each body or company required to have a DPO or that decides to appoint it, can then proceed to the selection of the DPO independently assessing the possession of the necessary requirements to perform the tasks to be assigned.

To work in Information Technology you need constant training because it is a sector with such rapid evolution that the knowledge acquired at the University will never be able to keep up with what is required by the labor market, which often seeks personnel with certifications attesting to the knowledge of determining technologies and languages.

Here are the 8/10 most requested certifications at this time:

1) (ISC) 2 CISSP, certifies the competence to design, implement and manage corporate security programs. Here is the non-profit website that promotes ISC certifications, recommended for those who want to work like: Security Consultant, Security Manager, IT Director/Manager, Security Auditor, Security Architect, Security Analyst, Security Systems Engineer, Chief Information Security Officer, Director of Security, Network Architect;

2) EC-Council's Certified Ethical Hacker, aims to form "ethical" hackers, able to counteract the activities of cybercrime;

3) Cisco CCNA (Routing and Switching), a reference point for network and network professionals where Cisco is the world's leading company;

4) The Open Group TOGAF 9.1 Certification, designed for the Togaf architecture of the same name, used by thousands of companies worldwide;

5) Microsoft MCSE: Cloud Platform and Infrastructure;

6) EC-Council's Certified Network Defender, a new certification introduced last year that certifies expertise in network security controls, risk and vulnerability assessment and the choice of appropriate firewall solutions to respond to any security incidents;

7) Microsoft MCSA: Windows Server 2016, serves to train professionals able to operate with the servers of this family, increasingly used in the IT field;

8) AXELOS PRINCE2 Foundation and Practitioner PRINCE2, is a certification in the field of Project Management that allows you to acquire all the tools that are essential to successfully complete a project;

9) Microsoft MCSD: App Builder, development of mobile applications, certifies the skills of professionals in designing and implementing the architecture of apps related to the house in Redmond;

10) CompTIA Security attests the ability to solve problems related to security events and operate within laws and regulations.

The first two most requested certifications are both in the field of security, a field in which it is a real emergency and the demand for this type of figure is constantly increasing.
In general, as IT security experts and DPO – Data Protection Officers, the most common (in term of market recognition) assessments and certifications are the UNI 11697:2017 Standard.

## Lithuania

In order to support the practical work of Data Protection Officers, which, under the EU General Data Protection Regulation, have been in place since 25 May 2018, it is imperative to have a large number of companies and all state agencies to attend special theoretical and practical training.

One of the key roles of the officer is to help monitor how the GDPR is being complied with within the company. For this purpose, the official may collect information, verify that the data processing activities meet the requirements, advise the controller or the processor, and make recommendations to him. Training of Data Protection Officers in Lithuania is being organized in accordance with the accredited PECB program. PECB is accredited according to ISO / IEC 17021, 17024, 17065 standards, and is accredited by international organizations IAS (International Accreditation Service), IAAR (The Independent Association of Accredited Registers), IPC (The International Personnel Certification Association).

The training material is provided, and the exam takes place in English. Usually such training is offered by private training institutions. The Data Protection Certificate is one way of demonstrating to both the employer, data subjects and the data supervisory authority that the Data Protection Officer has specific knowledge. DPC certificates are issued by national and international institutions such as associations of data protection professionals, universities, training institutes for civil servants, etc. One of these centers is located in Vilnius - CTG testing center. Certificates are usually issued after a training course and passing the relevant exam.

Having successfully passed the exam, you can apply for a CISM certificate.

Training for information security manual (CISM) is organized for experienced professionals. The CISM (Certified Information Security Manager) program is designed for experienced information security managers, managers, consultants, and employees directly responsible for information security management within the organization. This program is for those who develop, manage, maintain or evaluate information security. This certification shows that the information security specialist has the experience and knowledge to provide the appropriate management and consulting services. CISM defines core competencies and international performance standards to be met by those responsible for information security management. The CISM program is specifically designed for experienced professionals with expertise in information security management. CISM certification is for individuals who have been in charge of or have held similar positions and experience in the following areas for at least three years: combining an information security strategy with operational objectives; identifying and managing information security risk factors for performance targets; managing the information security program; developing and managing an incident and business continuity program. CISM Certified Professionals must: have a five-year (Information Security Manager - three years) experience in Information Security; pass an exam; to meet the annual requirements for further training. The course is based on international practices and standards[9].

Certification is a procedure where a learner receives a formal document from an authorized institution stating that he / she has achieved a certain qualification. Certification takes place after validation, as a result of issuing a positive decision stating that all learning outcomes required for a given qualification have been achieved. Certificates and other documents confirming the acquisition of qualifications should be recognizable and recognized in a given sector or industry. Validation is a multi-stage process of checking whether - regardless of how you learn - the learning outcomes required for a given qualification have been achieved. Validation precedes certification. Validation includes the identification and documentation of learning outcomes and their verification in relation to the requirements set for qualifications. Validation should be conducted in a fair and reliable manner.

[9] http://www.isaca.org/chapters1/Lithuania/sertifikacija/Pages/cism.aspx?utm_referrer=direct%2Fnot%20provided

## Poland

There is an Integrated Qualification System (*Zintegrowany System Kwalifikacji*) in Poland. The Minister of National Education, as the coordinator of the Integrated Qualifications System, in accordance with art. 51 par. 2 and 3 of the Act of 22 December 2015 on the Integrated Qualifications System (Journal of Laws of 2017, item 986, as amended), conducts and publishes a list of entities authorized to perform the function of external quality assurance towards certifying institutions. Entry of an entity on the list is made by way of an administrative decision after recruitment on the list (Article 52 (1) of the Act on the Integrated Qualification System).

The qualifications should be those that are broadcast in the system of education and higher education and those granted by public and local government authorities. However, in the scope of other qualifications important for the labour market, each institution decides whether to recognize a given document as confirming the qualification obtained on the basis of the above premises (validation, certification, recognition and recognition in a given area).

An example of a process leading to qualifications outside of the education and higher education systems is the adult vocational training provided by labour market institutions. Pursuant to the Act on the promotion of employment and labour market institutions (Journal of Laws 2004 No. 99 item 1001), vocational training of adults is a form of practical adult education or apprenticeships for adults, carried out without an employment relationship with the employer. This activation instrument must be implemented in accordance with the vocational training program including the acquisition of practical skills and theoretical knowledge and end with an examination confirming the qualifications in the profession.

Market qualifications (outside of education and higher education systems), are important in specific environments of social or professional activity and have their own validation and certification system. In addition, despite the lack of regulation by the Polish state, qualifications are also certificating for which a system for validation and certification of learning outcomes at the international level has already been developed.

Examples of qualifications in the area of information security and data protection are:

1) Computer / IT qualifications:

- Certificates of computer qualifications;
- European Profession Certificate Informatics at the basic level (EUCIP CORE);
- Oracle Java Certificate;
- Microsoft Certificates.

2) Financial qualifications:

- Qualified Bank Employee (Polish Bank Association);
- Certificate in risk management (Warsaw Banking Institute);
- Certificate of the WIB / ACI Polska Dealer (Warsaw Banking Institute);
- Certificate in the field of banking controlling (Warsaw Banking Institute);
- Certified Financial Consultant (Polish Bank Association);
- Specialist for Credit Analysis (Polish Bank Association);
- certificates in the field of financial consulting, based on the EFPA standard (European Financial Planning Association);
- ECB EFCB general bank certificate (EBTN / SSKBP) (Warsaw Banking Institute).

## 7. Reference list (incl. National Reports)

AMS - Austrian Labor Market Service (2016): IT - Informationstechnologie, available at: http://www.forschungsnetzwerk.at/downloadpub/edv1.pdf (02.01.2019)

AQA Agency for Quality Assurance and Accreditation (2016): Recognition of non-formally and informally acquired competences. available at: https://www.aq.ac.at (19.12.2018)

BayLDA (2016): EU-Datenschutz-Grundverordnung (DS-GVO), S. 1–2. Online verfügbar unter https://www.lda.bayern.de/media/baylda_ds-gvo_2_certification.pdf, zuletzt geprüft am 04.01.2019.

BKA - Bundeskanzleramt (2018) (ed): Informationssicherheitshandbuch, available at: www.sicherheitshandbuch.gv.at/ (18.12.2018)

Berg, Achim (2017): Der Arbeitsmarkt für IT-Fachkräfte. Hg. v. bitkom. Berlin. Online verfügbar unter https://www.bitkom.org/sites/default/files/pdf/Presse/Anhaenge-an-PIs/2017/11-November/Bitkom-Charts-IT-Fachkraefte-07-11-2017-final.pdf, zuletzt geprüft am 04.01.2019.

Blindert, Ute (2018): Heiß begehrt: IT-Security-Experten. DEKRA Arbeitsmarktreport 2018. Hg. v. karriereletter. Online verfügbar unter https://www.karriereletter.de/heiss-begehrt-it-security-experten-dekra-arbeitsmarkt-report-2018/, zuletzt aktualisiert am 17.07.2018, zuletzt geprüft am 04.01.2019.

BMEIA - Bundesministerium für Europa, Integration und Äußeres (2015): Informationssicherheitsgesetz aufgund EU-Verordnung (2015); available at: www.bmeia.gv.at (03.01.2019)

Brookson, Charles; Cadzow, Scott; Eckmaier, Ralph; Eschweiler, Jörg; Gerber, Berthold; Guarino, Alessandro et al. (2015): Definition of cybersecurity. Gaps and overlaps in standardisation. Heraklion: ENISA.

Bundesamt für Sicherheit in der Informationstechnik (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.

Bundesamt für Sicherheit in der Informationstechnik (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.

Bundesamt für Sicherheit in der Informationstechnik (2017): Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen, S. 1–14. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/VB-Personen.pdf?__blob=publicationFile&v=4, zuletzt geprüft am 04.01.2019.

Bundesamt für Sicherheit in der Informationstechnik (2018a): BSI - Kompetenzfeststellung und Zertifizierung von Personen. Hg. v. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Personenzertifizierung/personen_node.html, zuletzt geprüft am 04.01.2019.

Bundesamt für Sicherheit in der Informationstechnik (2018b): BSI - Schulungen anderer Anbieter. Hg. v. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/SchulungandererAnbieter/schulungandereranbieter_node.html, zuletzt geprüft am 12.01.2019.

Bundesamt für Sicherheit in der Informationstechnik (2018c): ISO 27001 Zertifizierung auf Basis von IT-Grundschutz. Hg. v. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Zertifizierung27001/GS_Zertifizierung_node.html, zuletzt geprüft am 04.01.2019.

Bundesamt für Sicherheit in der Informationstechnik (2019a): BSI - Schulungen anderer Anbieter. Hg. v. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/SchulungandererAnbieter/schulungandereranbieter_node.html, zuletzt geprüft am 04.01.2019.

Bundesamt für Sicherheit in der Informationstechnik (2019b): 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 (2015). European guidelines for validating non-formal and informal learning. Luxembourg: Publications Office. Cedefop reference series; No 104. available at: http://dx.doi.org/10.2801/669676 (10.01.2019)

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.

DIHK (2016): Deutscher Qualifikationsrahmen (DQR). IHK-Fortbildungsabschlüsse auf Hochschul-Niveau. Hg. v. DIHK. Online verfügbar unter http://ihk-bic.de/ihk-praxisstudium/deutscher-qualifikationsrahmen-dqr/, zuletzt geprüft am 12.01.2019.

DQR (2014): Liste der zugeordneten Qualifikationen. Hg. v. DQR. Online verfügbar unter https://www.dqr.de/media/content/Liste_der_zugeordneten_Qualifikationen_31_03_2014_bf.pdf, zuletzt geprüft am 12.01.2019.

DSB - Datenschutzbehörde der Republik Österreich (2019), available at: www.dsb.gv.at, (06.01.2019)

GDD (2018): Schulungen bei der GDD — GDD e.V. Das Ausbildungskonzept der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. Online verfügbar unter https://www.gdd.de/seminare, zuletzt geprüft am 04.01.2019.

Gutwirth, S; Leenes, R.; de Hert, P. (eds) (2015): Reforming European Data Protection Law.

IBW (2012): IT-Qualifikationen 2025. Analysen zu Angebot und Nachfrage. ibw Forschungsbericht Nr. 170, available at: www.ibw.at (08.01.2019)

IHK (2018a): 03_LK BAR | IHK-Projektgesellschaft mbH. Lotsendienst für Existenzgründer Landkreis Barnim. Hg. v. IHK. Ostbrandenburg. Online verfügbar unter https://www.ihk-projekt.de/unsere-projekte/national/02-lotsendienst-ff-los-um-und-bar/03-lk-bar/?L=0,https://www.ihk-bildungszentrum-cottbus.de/details.jsp?ver_id=2330, zuletzt geprüft am 04.01.2019.

IHK (2018b): IHK Bayreuth-Bildungskatalog 2018.2. Die Weiterbildung für Oberfranken (2), S. 1–156. Online verfügbar unter https://www.bayreuth.ihk.de/upload_ihk_alless01/IHK_Bildungskatalog_2018_2_439350.pdf, zuletzt geprüft am 04.01.2019.

IHK (2018c): Sachliche und zeitliche Gliederung der Berufsausbildung. Anlage zum Berufsausbildungsvertrag, S. 1–17, zuletzt geprüft am 04.01.2019.

IHK (2018d): 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.

IHK (2019): Das IHK-Netzwerk - IHK. Hg. v. IHK. Online verfügbar unter https://www.ihk.de/wir-uber-uns, zuletzt geprüft am 12.01.2019.

IHK Bayreuth (2018): IHK Bayreuth-Bildungskatalog 2018.2. Die Weiterbildung für Oberfranken, S. 1–156. Online verfügbar unter https://www.bayreuth.ihk.de/upload_ihk_alless01/IHK_Bildungskatalog_2018_2_439350.pdf, zuletzt geprüft am 12.01.2019.

Klebl, Ulfried; Nerdinger, Friedemann W. (2010): Kompetenzentwicklung durch Development-Center. In: *Zeitschrift für Arbeits- und Organisationspsychologie A&O* 54 (2), S. 57–67. DOI: 10.1026/0932-4089/a000012.

KPMG (2013): Study on Austrian Information Security Awareness, available at: www.kpmg.at (28.12.2018)

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.

Mesmer, Alexandra (2018): Softwareentwicker, Security-Experten und Berater besonders begehrt. Hg. v. Computerwoche. Online verfügbar unter https://www.computerwoche.de/a/softwareentwickler-security-experten-und-berater-sind-besonders-begehrt,3545136, zuletzt aktualisiert am 11.06.2018, zuletzt geprüft am 04.01.2019.

NQS (2016): Handbuch für die Zuordnung von Qualifikationen zum NQR. Online verfügbar unter: https://www.qualifikationsregister.at/wp-content/uploads/2018/11/HandbuchNQR.pdf (06.01.2019)

Whitten, Dwayne (2008): The Chief Information Security Officer. An Analysis of the Skills Required for Success. In: *Journal of Computer Information Systems* 48 (3), S. 15–19. DOI: 10.1080/08874417.2008.11646017.

Wikipedia (2019a): Information privacy. Hg. v. Wikipedia. Online verfügbar unter https://en.wikipedia.org/w/index.php?oldid=873938916, zuletzt aktualisiert am 31.12.2018, zuletzt geprüft am 04.01.2019.