# Desk Research Austria

| **Document Details:** | |
|---|---|
| Reference | **TeBeISi** |
| IO / Activity | IO1 – Desk research |
| Author(s) | Schober, P.; Cammerlander, L. |
| Character | Country Report Austria |
| Date | 15.01.2019 |

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

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

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

.

Funded by the
Erasmus+ Programme
of the European Union

## Table of Content

Funded by the
Erasmus+ Programme
of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

## 1. Aim of the 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 training providers 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. Next qualification offers covering this topic will be identified and their suitability will be estimated. Furthermore, the current demand of the labour market in terms of available job offers and the acquired competences will be described. Against this background a possible profile for Information Security Officers and Data Protection Officers will be drafted 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** means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms. (Wikipedia 2019b)

**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).

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

## 2. National Rules & Regulations Concerning Information Security and Data Protection in SME & Nonprofit Organizations

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)

### 2.1 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.

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

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

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

### 3.1.NQR in Austria

The aim of the National Qualifications Framework (NQF) is 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.

The qualifications available in Austria are classified in the NQR according to Figure 1 (NQS 2016):

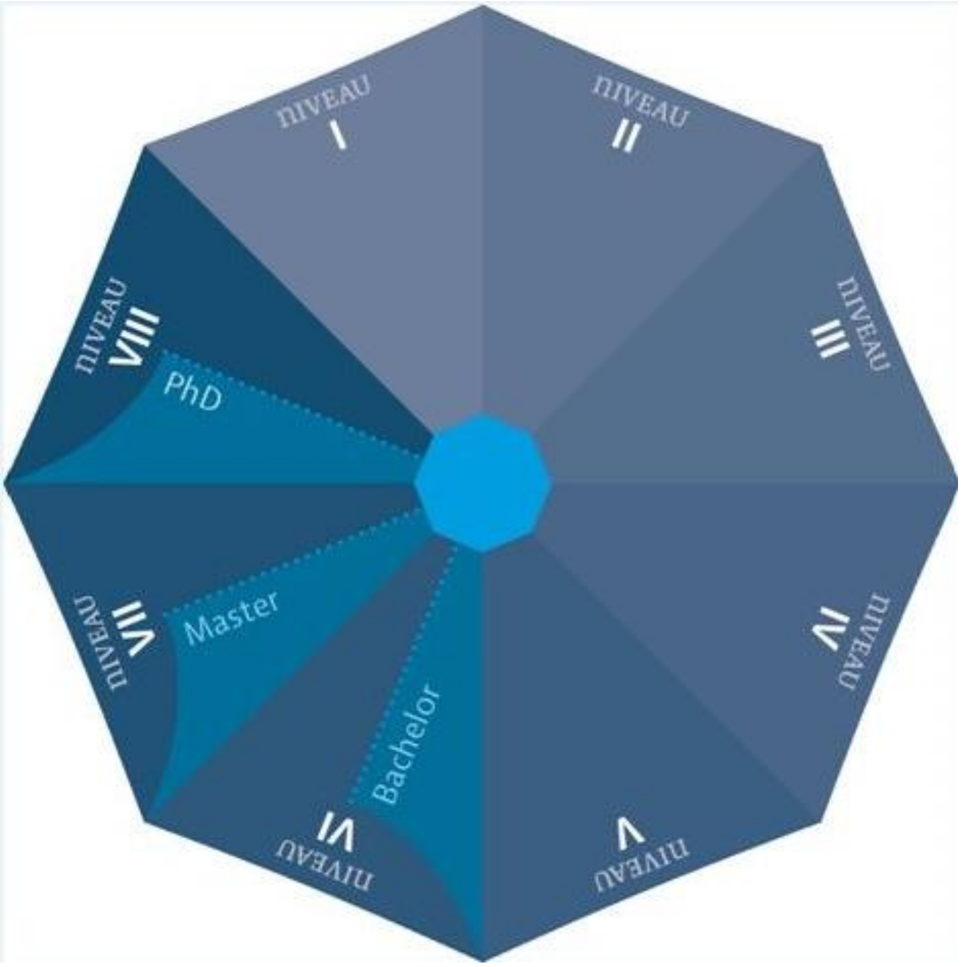

*Figure 1: NQR in Austria - Source: NQS (2016)*

According to this schedule, training and accreditation for Information Security and Data protection can be seen in level IV or level V (depending on prerequisites of individual participants.

Funded by the Erasmus+ Programme of the European Union

## 3.2.ICT vocational training in 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).

Funded by the
Erasmus+ Programme
of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

### 3.3. Overview of Existing Training Offers in the Field of Information Security

| Name of Training Course | Main Content / Objective | Target Groups (basic /intermediate / proficient user) | Skills acquired (professional, social and transversal) | Kind of Testimonial |
|---|---|---|---|---|
| Information Security basics | The seminar provides an insight into the topic of information security.<br>It explains terms such as "data" and "information security", and gives an overview of the current standard series ISO 27000. After the seminar, the contents of an information security management (ISMS) are understood. One is capable of the potential security needs of the company and can identify solutions for the protection of corporate information. | Entrepreneurs, managers, decision makers, QM and prospective DS Officer, interested parties | • Recognizing the real threats from criminals operating in the network;<br>• Recognition of social engineering attacks;<br>• Knowledge of security principles and proper behaviour while using computers and other ICT equipment, in particular when using Internet services. | |
| Information Security Manager | Information security managers occupy the central position in a company in which leadership and technology competence are equally in demand. They are responsible for the establishment, implementation and continuous improvement of the Information Security Management System (ISMS) and act as an interface between the top management and the operating divisions.<br>(Reference: http://at.cis-cert.com/Ausbildungen/Informationssicherheit/IS-Manager/Information-Security-Manager-ISO-27001.aspx, 27.12.2018) | Entrepreneurs, managers, decision makers, computer scientists, computer officers, IT experts and whoever is interested | • Knowledge about the basics of the information security system;<br>• Skills of implementing the acquired technical knowledge in the company;<br>• The ability to work in a team and to resolve conflicts;<br>• • Knowledge of the basics of law. | Nationally and internationally recognized certificate "Information Security Manager in accordance with ISO / IEC 27001". |
| Information Auditor | The series of courses to the IS auditor is the ideal complement for trained IS managers. As an auditor, all internal audits can be carried out by themselves and the company prepared itself for external audits with the help of the course-mediated methods. The IS auditor in the company is the "supreme authority" for ISM systems. It assesses the information security to their conformity to | Information Security Manager<br>(To participate, a valid certificate as an IS manager is needed. In this way a high level of | • Acquainting with the provisions of the regulation on the protection of personal data;<br>• Knowledge of how to adapt the organization to new regulations; | Nationally and internationally recognized certificate "Information Security Auditor |

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

| | | | | |
|---|---|---|---|---|
| | standards and identifies potential improvements before a company will be certified with the CIS certificate for the best possible standard of safety according to ISO / IEC 27001 or given an extension. (Reference: [http://at.cis-cert.com/Ausbildungen/ Informationssicherheit/IS-Auditor/Information-Security-Auditor-ISO-27001.aspx,](http://at.cis-cert.com/Ausbildungen/Informationssicherheit/IS-Auditor/Information-Security-Auditor-ISO-27001.aspx) 27.12.2018) | qualification of the auditors is ensured.) | • The ability to develop and implement an internal security policy;<br>• The ability to assess risk;<br>• The ability to solve typical problems related to personal data. | for ISO / IEC 27001" |

Funded by the Erasmus+ Programme of the European Union

### 3.4. Overview of Existing Training regarding Data Protection

| Name of Training Course | Main Content / Objective | Target Groups (basic /intermediate / proficient user) | Skills acquired (professional, social and transversal) | Kind of Testimonial |
|---|---|---|---|---|
| Preparatory Training as a data protection officer | With this seminar the skills necessary to master the future role as Data Protection Officer are obtained. All relevant legal and technical knowledge is provided and the goal of the seminar-workshop is to be "practical proof" in data protection. After the seminar one will have the ability to sense the data protection issues and to control them within the company. One has the communicative ability of the data protection rules to mediate in the company and one feels grown to the entire tasks of a Data Protection Officer.<br>(Reference: http://www.kmu-plattform.eu/betrdaten.html, 12.12.2018) | Future data protection officers, engineers, lawyers, managers and interested parties who wish to obtain a thorough overview on the issue of data protection officer. | • Knowledge about the basics of data protection;<br>• • Knowledge of the basics of law. | Certificate of attendance |
| data protection officer | SOUND LEGAL BASIS<br>DATA PROTECTION OFFICER<br>Forms of the DSB<br>Internal or External? Role conflict with creation of systems?<br>assignments<br>DATA PROTECTION IN AUSTRIA<br>Austrian Adaptation Act 2018<br>data protection authority<br>DATA PROTECTION IN THE COMPANY<br>Action plan and procedure<br>risk assessment | Corporate data protection officers, managing directors, heads and employees of IT departments, IT security officers, HR officers, compliance officers, works council members, consultants | • Legal knowledge on GDPR<br>• Knowledge about role and responsibilities of an DPO<br>• Knowledge on Risk management strategies<br>• Ability to resolve conflicts of interest; | "Data Protection Officer" of Austrian Standards based on the international standard ISO/IEC 17024 |

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

| | | | | |
|---|---|---|---|---|
| | TECHNICAL AND ORGANISATIONAL MEASURES (Reference: https://www.tectrain.at/seminare/themen , 10.01.2019) | | | |
| Preparation for EU Data Protection Regulation | Data protection is a fundamental right. For this reason, the basic EU data protection regulation describes obligations for companies. In this training to become a data protection officer, you will deal with the legal basis and legal necessities. What you can expect: Practical knowledge for setting up a legally compliant data protection management system.. (Reference: https://www.wifi.at/ 20.12.2018) | Decision-makers from business, public authorities, public corporations, employees in the fields of data processing, data protection and IT security, legal, auditing and controlling departments as well as personnel and organizational managers. | • data protection law<br>• Basic legal knowledge<br>• Data Protection Act DSG 2000, EU Data Protection Basic Regulation<br>• data security engineer<br>• Tasks, role, rights and obligations<br>• Statutory audit instruments<br>• New supervisory authority, etc.<br>• Implementation in the company<br>• Development of a data protection management system<br>• Introducing EU-DSGVO data protection standards, making default settings, identifying risks and vulnerabilities, impact assessment<br>• Rights and duties<br>• Information duties, accountability, rights of data subjects and their implementation<br>• Technical data protection and IT security<br>• Preferences, Privacy by Design and Privacy by Default,<br>• Contractual data protection | Data Protection Officer" of Austrian Standards based on the international standard ISO/IEC 17024 |

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

| | | | | |
|---|---|---|---|---|
| | | | - Preparation of the procedure directory, role concept and user agreement | |

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

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

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).

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

### 4.1. Overview of job offers in the field of Information Security

| Job offer / enterprise | General description | Skills required (professional, social and transversal) | Link |
|---|---|---|---|
| **Information Security Officer** | Ensuring information security in critical infrastructures (e.g. smart metering)<br>Development and operation of an Information Security Management System ISMS<br>Implementation of risk management for the Smart Meter program and risk audits<br>Conception and control of emergency and crisis management, participation in crisis exercises<br>Monitoring of the legal regulations under the focus of the effects on the Viennese networks | Completed technical education (university/technical college specialising in computer science, information security, business informatics, HTL with relevant professional experience in the field of ICT security)<br>Experience as Information Security Officer and knowledge of current regulations in the ICT security environment (BSI, ISO 27001)<br>Practical experience with communication technologies such as mobile radio, short-range radio, power line communication is an advantage.<br>Fluent in English<br>High sense of responsibility and integrity<br>Communication and team skills | https://www.wienernetze.at/ |
| **Information Security Analyst** | Provide guidance and help to protect and secure our intellectual property<br>Create specific protocols that audit file changes such as updates, deletion, additions and moving<br>Penetration testing and monitoring of current digital assets<br>Perform risk analysis to identify any security issues that could lead to lost or stolen data<br>Monitor current security alerts to patch software such as operating systems with the latest versions<br>Identify security breaches and take action to stop them and prevent them in the future<br>Implement the right software and hardware into current and future network environments<br>Working in an international team and environment<br>Participate in development of our information security management framework | Bachelor degree in a relevant field (e.g. Information Security) or information security related experience<br>Knowledge of good practice and standards for example ISO27000 Series, Cobit 5. etc.<br>Experience with scripting languages Phyton, Perl, etc.<br>Knowledge of web technologies like HTTP, JS, PHP, JAVA, simple networking<br>Basic knowledge of operating systems Windows 7,10, Windows Server 2012 R2, 2016 as well as Debian and Ubuntu Linux<br>Fluent English (written and spoken) and a willingness to learn the local language<br>Must be willing to travel occasionally<br>Experience working in a complex, global environment | https://www.sportradar.com/ |

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

| | | | |
|---|---|---|---|
| | Automate our application and infrastructure scanning and reporting<br>Further development of our information security awareness program | Information security certifications (CISSP, CISM, CISA, etc.) are considered as a plus | |
| Information Security Analyst | Support for the Security Operations Centre (SOC) team. The SOC Analyst/ Incident Handler will provide advanced support for monitoring alerts in a global enterprise during critical and high-volume events; responding to security incidents according to established policies and best practices; providing guidance to other Analysts and other first responders for the proper handling of information security incidents; coordinating efforts and providing timely updates to business units during response and providing recommendations as required; opening tickets for incidents and tracking to completion; coordinating the flow of information between different business units within the enterprise and communicating clearly the status of incidents to senior management. This position requires the ability to work a regularly scheduled day shift with availability after hours depending on need | •3+ years' experience working in a SOC or equivalent analyst experience<br>•Experience with event escalation and reporting procedures to support investigations<br>•Experience leading teams during incident investigations and remediation<br>•Advanced knowledge of SIEM platforms such as Splunk, QRadar, ArcSight, ELK, etc.<br>•Knowledge of TCP/IP and common protocols and applications, including DNS, HTTP, SMB, FTP, SMTP, SNMP and associated encrypted protocols<br>•Knowledge of network monitoring, analysis and troubleshooting techniques<br>•Knowledge of security controls such as firewalls, IDS's, AV and content filtering<br>•Knowledge of how the Windows file system and registry function<br>•Familiar with malware, ransomware and phishing techniques<br>•Ability to demonstrate analytical expertise under pressure, and to learn and adapt quickly<br>•Ability to collaborate with different teams and communicate clearly<br>•Bachelor's degree in Computer Science, Cyber Security or other tech-related field<br>•Experience with common incident response tools<br>•Knowledge of cyber threat and technical capabilities to defend networks and systems<br>•Ability to inform or brief management and senior leadership, when appropriate<br>•Possession of excellent oral and written communication skills; ability to clearly and | https://www.fortinet.com/corporate/careers/careers.html |

Funded by the
Erasmus+ Programme
of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

| | | | |
|---|---|---|---|
| | | concisely document security incident details and escalate appropriately, when required<br>•Possession of excellent initiative and critical thinking skills | |
| Information-/IT-Security-Officer | (Further) development, roll-out and control of guidelines and guidelines for the protection of information and IT systems<br>Advising the Executive Board on IT security issues<br>Training and awareness of employees<br>Processing, evaluation and documentation of information security relevant incidents<br>Cooperation in IT security projects within ERGO Austria and in the ERGO Group environment (Germany) | IT-specific training, studies with focus on IT security preferred<br>2 to 3 years of professional experience in the field of information/IT security would be an advantage<br>relevant expertise in the field of technical and organisational information security measures<br>good knowledge of German and English<br>absolutely reliable and structured working method<br>quick comprehension, especially recognition of connections and dependencies<br>innovative and networked thinking personality<br>distinct ability to communicate and work in a team | https://ergo-versicherung.at/ueber-ergo/karriere/ |

Funded by the Erasmus+ Programme of the European Union

### 4.2. Overview of job offers in the field of Data Protection

| Job offer / enterprise | General description | Skills required (professional, social and transversal) | Link |
|---|---|---|---|
| **Senior Manager Group Data Protection** | Support of the Group Data Protection Officer in advising data protection law as well as advising our locations.<br>Independent support of the departments in questions of operational data protection compliance, among other things with regard to data protection-relevant business processes<br>Proactive consulting in the technical implementation of data protection requirements (Privacy by Design)<br>Independent data protection support and accompaniment of projects<br>Advice on data protection law for the specialist departments in product design. | Completed study of law<br>Relevant professional experience, of which 2-3 years in the field of data protection<br>Ideally, in-depth IT knowledge, in particular in the area of applications in a corporate environment, as well as knowledge of common security standards<br>Structured, analytical approach<br>Strong communication and assertiveness as well as ability to work in a team<br>Very good knowledge of written and spoken English<br>Excellent knowledge of German at mother tongue level | https://www.karriere.at |
| **Data Privacy Counsel** | The Data Privacy counsel will be the leading expert and centre of competence on data privacy matters:<br><br>Maintain Global Red Bull Data Privacy Framework<br>Maintain and further develop data privacy compliance strategy<br>Liaise with other departments, especially IT, in order to achieve high standards of technical and organisational data protection<br>Maintain overview of data landscape within Red Bull (data mapping exercise)<br>Conduct privacy impact assessments for existing and new applications/tools | Minimum of 5 years of professional experience in an international law firm or as in-house counsel of an international company<br>Relevant experience in a similar role and/or experience of working in or with technology and/or media businesses with significant consumer facing social media activity and content is a prerequisite<br>Extensive knowledge of data privacy laws (esp. GDPR and the respective national implementation laws), consumer protection laws and basic IT knowledge (data processing and storage, databases and computer systems).<br>Professional communication and presentation skills | https://www.redbull.com/at-de |

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

| | | | |
|---|---|---|---|
| | Further develop Red Bull Data Retention Framework<br>Ensure global alignment and file registrations with data protection authorities Keep Global Data Transfer Agreement updated<br>Build up and maintain knowledge and expertise on data protection issues, technical developments and changes of the legal setting globally | Excellent analytical and organizational skills, proactive working style<br>Excellent organizational skills and process-oriented, well-structured working style<br>Ability to work in a fast paced environment and towards tight deadlines<br>Loyal and reliable team player | |
| **Data Security Specialist** | Information Security Administrator in the scope of GDPR<br>Reviewing contracts and procedures for information processing<br>Testing processes for ensuring safety<br>Participation in projects regarding the processing of personal data and adaptation of the Company to the GDPR<br>Development of in-house procedures related to personal data processing policy and responsibility for their implementation<br>Conducting training in the field of data security | Higher education, preferred law or administration<br>Experience in a large organization with a structured structure<br>Basic knowledge of personal data protection regulations<br>Basic knowledge of standards in the area of information security<br>Experience in independent project management<br>Interpersonal skills | https://www.karriere.at |
| **Team lead IT Infrastructure & Data Security** | Operation of the entire IT infrastructure of the international group of companies including support with a 5-person internal team and the 24/7 service desk, which is outsourced to an external partner.<br>Development of a centrally controlled corporate network based on Aruba and FortiGate network components<br>Set-up of a group-wide SD-WAN<br>Implementation of the "Cloud First" strategy based on MS Azure<br>Implementation of a state-of-the-art data security concept | At least 3 years of experience in a coordinating position in a complex IT infrastructure environment, either in the Group IT of an international group or with an IT service provider.<br>Profound network know-how, preferably on the basis of Aruba and FortiGate<br>Extensive experience with server operation in MS Azure<br>Comprehensive knowledge in the field of Information Security<br>Change management approach and communicative personality<br>Good command of spoken and written English | https://www.karriere.at |

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

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

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.

## 6. Other important issues

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

The responsibility for IT security always lies with the management according to the Commercial Legal Code (UGB) and the GmbH Act (GmbHG).

Even if security-relevant IT tasks are handed over to employees, the company management is ultimately responsible for compliance with the legal regulations.

The EU Basic Data Protection Regulation (DSGVO) and the Austrian Data Protection Act regulate the handling of personal data (e.g. name, date of birth, e-mail address, IP address).

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

Companies must take appropriate technical and organisational measures (e.g. data backup, encryption, access controls) to protect data from accidental destruction, data loss or unlawful use by third parties.

Funded by the
Erasmus+ Programme
of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

## 7. Executive Summary and Resume

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.

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

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.

One of the reasons might be the fact, that 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)

Additionally it is to mention, that in Austria, the areas of information security and data protection are strictly regulated by law.

The responsibility for IT security always lies with the management according to the Commercial Legal Code (UGB) and the GmbH Act (GmbHG).

The EU Basic Data Protection Regulation (DSGVO) and the Austrian Data Protection Act regulate the handling of personal data.

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

## Reference list

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 (19.112.2018)

Berg, Achim (2017): Der Arbeitsmarkt für IT-Fachkräfte. Hg. v. bitkom. Berlin. available at: https://www.bitkom.org/sites/default/files/pdf/Presse/Anhaenge-an-PIs/2017/11-November/Bitkom-Charts-IT-Fachkraefte-07-11-2017-final.pdf (12.01.2019)

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

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

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)

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

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)

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

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)

Wikipedia (2019a): Information privacy. Hg. v. Wikipedia. available at: https://en.wikipedia.org/w/index.php?oldid=873938916, (05.01.2019)

Wikipedia (2019b): Information security. Hg. v. Wikipedia. available at: https://en.wikipedia.org/w/index.php?oldid=876029889, (05.01.2019)

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.