WYŻSZA SZKOŁA
Biznesu i Nauk o Zdrowiu w Łodzi

TeBeISi

Desk Research Poland

Document Details:	
Reference	**TeBeISi**
IO / Activity	IO1 – Desk research
Author(s)	Prof. Wojciech Welskop, PhD
Character	Country Report - Poland
Date	07.01.2019

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

.

Funded by the
Erasmus+ Programme
of the European Union

Table of Content

1. Aim of the Report 3

2. National Rules & Regulations Concerning Information Security and Data Protection in SME & Nonprofit Organisations 5

3. Vocational and Continuing Education and Training in this area 7

3.1. Overview of Existing Training Offers in the Field of Information Security 9

3.2. Overview of Existing Training Regarding regarding Data Protection 12

4. Overview of jobs offered in the field of Information Security and Data Protection 15

4.1. Overview of job offers in the field of Information Security 16

4.2. Overview of job offers in the field of Data Protection 22

5. Existing Methods for Assessing and Certification of Vocational Skills aquired outside formal Education 28

6. Other important issues regarding the topic of the report 30

7. Executive Summary and Resume 31

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 traing providers and the demands and needs of the labor 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. Further more the current demand of the labor 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.
(Reference: http://en.wikipedia.org/wiki/Information_security, 04.11.2018)

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.

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)

National Rules & Regulations Concerning Information Security and Data Protection in SME & Nonprofit Organisations

The security assurance of data and information is a key challenge for companies in the 20th and 21st centuries. Due to a widespread use of IT and the IT supported storage and processing of data, the issue concerns mainly the new technologies. Legal regulations, norms and good practices that are included in various management methodologies constitute signposts when analyzing and solving the complexity of the issue. The results of the analysis of these documents from the point of view of particular public administration entities or companies that protect their resources should be given in a document referred to as the Information Security Policy.

The obligation to protect data also results from legal provisions that define the requirements for how to protect this information. 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);
- 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);

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.

- 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,

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.

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][1], 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[2], 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[3], 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. Vocational and Continuing Education and Training in this area

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. 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

[1] 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] (Th e Offi cial Journal of the European Union L.2016.119.1).

[2] *Journal of Laws No. 78, item 483.*

[3] *Journal of Laws 2014, Item 121 with amendments.*

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.

and Data Protection. In Poland there are a lot of trainings in the field of Information Security and Data Protection.

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.

2.1. Overview of Existing Training Offers in the Field of Information Security

Name of Training Course	Main Content / Objective	Target Groups (basic /intermediate / proficiant user)	Skills acquired (professional, social and transversal)	Kind of Testimonial
Basic training in information security	Presenting participants with security threats and methods of protection against them; presentation of ways to protect valuable information from disclosure and improper use by competitors, employees or contractors; raising the level of participants' awareness about the presence of threats to information in the organization.	Basic user	• Recognizing the real threats from criminals operating in the network; • Recognition of social engineering attacks; • Knowledge of security principles and proper behavior while using computers and other ICT equipment, in particular when using Internet services.	Certificate of participation
Risk management in Information Security Systems in accordance with ISO / IEC 27005: 2011	Acquiring knowledge on identifying and analyzing information security risks as well as procedures and control mechanisms used to avoid risks.	Basic user	• Knowledge of terms and definitions in the area of information security; • The ability to recognize the typical information security risk in an organization; • The ability to recognize common problems of managing information security risks; • The ability to assess the threats to information assets; • The ability to identify, analyze and	Certificate of participation

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.

			assess information security risks	
BI_CRISC CRISC - Certified in Risk and Information Systems Control	The training aims to prepare participants to pass the Certified in Risk and Information Systems Control, conducted by the ISACA association.	Proficiant user - persons performing the duties of auditor of IT systems in their organizations or intending to take the CRISC exam.	The CRISC preparation course includes 5 areas of activity appropriate for the Manager, who was entrusted with the risk management of information processing: Area 1 - Risk identification, analysis and evaluation Area 2 - Risk response Area 3 - Risk monitoring Area 4 - Designing and implementing security Area 5 - Monitoring and maintenance of security	Certificate of participation
Information Security Manager according to ISO 27001 - accredited training	Acquiring knowledge about the processes and requirements related to the implementation of ISO 27001 and ISO 27002 standards in the company and their practical application. Acquiring knowledge in the field of law and psychology to efficiently and in accordance with regulations introduce the acquired technical knowledge in the company.	Intermediate user	• Knowledge about the basics of the information security system; • Skills of implementing the acquired technical knowledge in the company; • The ability to work in a team and to resolve conflicts; • Knowledge of the basics of law.	International Certificate of Information Security Manager ISO 27001

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.

Information security management system in accordance with PN-EN ISO / IEC 27001: 2017-06	The training aims to familiarize with the subject of information security, requirements of the standard as well as the approach to the implementation of the information security management system.	Intermediate user	• Knowledge about information security; • Knowledge about the information security management system; • The ability to implement the information security management system in the company.	Certificate of participation
Introduction to information security	Participants will learn about the current threats to systems and data, as well as on how to increase security in the company.	Basic user	• Understanding the threats affecting the organization's operations and finances; • Learning basic risk estimation techniques; • Learning techniques for securing computer networks and electronic data.	Certificate of participation
Internal auditor of the information security management system ISO / IEC 27001: 2017	Acquiring the skills and knowledge needed to conduct internal audits of the information security management system ISO / IEC 27001: 2017.	Proficiant user	• Knowledge about information security; • Competences of internal aditors; • The ability to plan internal audits, prepare for the audit, conduct audit activities, audit documentation and audit reports; • Verbal and non-verbal communication skills in the audit.	Certificate 'Internal Auditor ISBI ISO / IEC 27001: 2017'

2.2. Overview of Existing Training Regarding regarding Data Protection

Name of Training Course	**Main Content / Objective**	**Target Groups (basic /intermediate / proficiant user)**	**Skills acquired (professional, social and transversal)**	**Kind of Testimonial**
Course for Data Protection Inspectors	The aim of the course is practical preparation for independent performance of the duties of the Data Protection Officer.	Intermediate user - the course is addressed to current as well as future Data Protection Inspectors, as well as to persons responsible for information security	• Acquainting with the provisions of the regulation on the protection of personal data; • Knowledge of how to adapt the organization to new regulations; • The ability to develop and implement an internal security policy; • The ability to assess risk; • The ability to solve typical problems related to personal data.	Certificate of participation
Data Protection Inspector	The aim of the training is to provide the most practical knowledge, enabling independent performance of the Information Security Administrator (and after changing the EU regulations - the Data Protection Officer).	Basic user	• Knowledge about the responsibilities of the Information Security Administrator; • The ability to train employees; • Knowledge of changes resulting from the EU Regulation on the protection of personal data.	Certificate of participation
Comprehensive	The aim of the training is to	Basic user	• Knowledge of the law and their	Certificate of

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.

Training for Data Protection Inspectors	provide comprehensive knowledge necessary for the future Data Protection Inspectors in performing their function.		practical implementation; • The ability to analyze risk; • Knowledge of organizational and technical measures ensuring the security of personal data processing; • Knowledge of practical aspects of implementing changes in the organization.	participation
RODO (ang. GDPR) 2018 - the most important changes in the provisions on the Protection of Personal Data	The aim of the training is to learn the legal basis in the field of personal data, concepts used in current legislation.	Basic user	• Knowledge of the legal basis in the field of personal data; • The ability to determine if the information obtained is personal data; • The ability to respond to cases of violations.	Certificate of participation
ISO / IEC 29151: 2017 Practical rules for securing personal data	The aim of the course is to support organizations that process personal data in the appropriate selection of security measures to identified privacy risks.	Intermediate user	• The ability to plan appropriate safeguards for the organization that processes personal data; • The ability to test and implement security in all organizational processes; • The ability to justify the choice of specific safeguards for the protection of personal data.	Certificate of participation
Role and duties of the Inspector of Data Protection in the organization	The aim of the training is to get to know the role of the Data Protection Supervisor in the organization.	Intermediate user	• Expert knowledge on data protection; • The ability to resolve conflicts of interest;	Certificate of participation

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 ability to analyze risk.	
Certified Inspector of Protection Personal Data	The aim of the training is to familiarize the participants with the regulations - in terms of legal and organizational-technical aspects.	Intermediate user	• Knowledge of the areas of data processing; • The ability to select the appropriate technical and organizational security; • The ability to develop a security policy procedure and IT system management instructions.	Certificate of participation

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

The effectiveness of any security-focused job depends on clear definitions of roles and strong communication up and down the line as to the tasks and responsibilities for which each player is responsible. Crafting a good information security and data protection jobs sdescriptions is a big challenge, because each company has different needs and has its own expectations for each role on the security team. This report summarizes information on employment of job offers in the field of Information Security and Data Protection in Poland.

3.1. Overview of job offers in the field of Information Security

Job offer / enterprise	General description	Skills required (professional, social and transversal)
Information Security Specialist / Eurobank	• Conducting and coordinating risk analysis for information security in the area of IT infrastructure, and supporting other shareholders in preparing the contribution to risk analysis in the field of information security. • Business support in decision making by providing risk analysis in the field of information security and participation in the project process in the scope of defining guidelines and controlling compliance with safety requirements. • Coordinating the risk assessment of the Bank's IT systems and recommending recovery plans in the field of information security, including IT infrastructure security. • Coordination of creating risk analysis documents and security level (eg Security File etc.) of IT systems, applications, and business processes and initiatives. • Consulting projects, business initiatives, procedures, contracts with external partners, results of security tests, etc. • Support in servicing audit missions,	• 2 years of work experience in a position related to the analysis of the risk of IT infrastructure security. • Good knowledge of the best security architecture practices • Good knowledge of infrastructure components, including infrastructure security components (eg network security, firewalls, IDS, IPS) • Good knowledge of the best security architecture practices (ISO 27001, CobiT, ITIL) • Experience in risk assessment in the area of information security or conducting audits • Independence, good organization of work and the ability to work under time pressure • Very good knowledge of the MS Office package • Knowledge of English at least B1 (Intermediate)

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.

	inspections, regulatory, corporate and internal controls. • Support in the dissemination and development of proposals for educational and training initiatives that raise the awareness of employees and business partners	
Expert on Protected Information Security / BGK State Development Bank	• Preparation and implementation of internal normative acts regarding the principles of information processing and protection • Controlling compliance with the rules of information processing protected in terms of the adequacy of the level of security and daily monitoring of external information leakage • Reviewing draft internal normative acts and contracts in terms of their compliance with requirements in the area of information security • Providing consultations to the Bank's employees regarding the principles of information processing and preparing documents containing legally protected information • Conducting trainings at the Bank regarding the rules for processing protected information	• Higher education - the preferred course of law, information security or related • About 4 years of experience related to the information security area • Minimum 1 year of experience in the analysis of events related to information leakage as part of the Information Security Management System • Experience in the field of data exchange analysis in the organization • Knowledge of information classification systems • Knowledge of standards is welcome: 27001 Information security management systems, 27002 Practical information security principles, 27005 Information security management in information security • Knowledge of the Windows 7 and 10 operating system and the Office suite • English at the level of reading technical documentation • Ability to think analytically • Communicativeness, openness, ability to cooperate in a team • Independence in action and ability to organize own work

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.

Specialist for information security / BGŻ BN PARIBAS	• Development of standards and regulations in the field of information security and information systems; • Reviewing draft internal banking regulations in the field of information security and information systems; • Reviewing solutions in the area of information security and teleinformation systems; • Reviewing agreements in the field of information security; • Performing security risk analysis; • Preparing and conducting training in the field of security; • Conducting special investigations in the event of information security breaches.	• Higher education; • 3 years of professional experience in the area of information security; • Knowledge of English at a level that allows free communication in the form of oral and written; • Interest in the information / IT security area; • Analytical skills - obtaining information from many sources, preparing reports and documentation; • Independence and willingness to develop; • Good work organization and commitment; • Expert MS Excel service; • Knowledge of security standards - standards ISO / IEC 27001, NIST and the requirements of KNF, RODO.
Information security specialist / NETIA	Advice related to information security, in particular regarding data processing and management: personal, constituting a telecommunications secret, being the company's secret.	• Master's degree education, preferred specializations: legal, administration, management - with particular emphasis on personal data, • knowledge of legal provisions regarding the protection of personal data, information security and telecommunications law, • experience in the application of the law on the protection of personal data, including in the scope of their processing in information systems, • independence, creativity and responsibility in the implementation of tasks, • business and / or technological industry knowledge

		(telecommunications) will be an advantage.
Cyber Security Risk Assessor / CREDIT SUISSE Poland	• You will have a superb opportunity as Cyber Security Risk Assessor within the CISO Switzerland, Swiss Universal Bank and International Wealth Management department. • You will have the responsibility to execute in-depth security assessments for the bank's most meaningful projects and business applications as well as for legal entities and branches including the option to travel from time to time. • An expert role responsible for providing security consultancy and standard methodology advice within IT and business project teams. • You will have an unusual chance to support and drive a variety of initiatives and programs in the area of cyber and information security. • Opportunities to improve assessment methodologies and processes in collaboration with other business partners in the global Chief Information Security Officer (CISO) organization. • Excellent career development/growth equal opportunities within the global CISO organization.	• Preferred 3-4 years broad experience in information and/or cyber security, ideally within a larger organization. • Professional certifications in information/cyber security (e.g. CISSP/CISA/CISM) are an advantage. • Do you have IT Security audit or risk assessment experience in complex IT environments are helpful? • Is uncovering weaknesses in processes and technology is your passion? • Are you a great teammate with excellent analytical skills, problem solving and good communication skills? • You are fluent in English, both written and verbal.
Chief Information Security Specialist	We are a company supporting the Capital Group in application management as well as IT	• higher IT education or related,

/ Energa Informatyka i Technologie Sp. z o.o.	infrastructure, we also provide information security services, we provide the User's work position (e-Workplace) and we build IT solutions in the field of software development for the needs of our Organization.	• minimum 4 years of experience in administering Windows or Linux family systems, • a minimum of 4 years of practice in the identification and analysis of incidents that may affect • for the security of IT services, • knowledge of issues and technologies related to behavioral analysis and detection of unusual actions and behaviors of users and devices in corporate networks, • knowledge of issues in at least one area of the area: analysis of Malware, reverse engineering / programming / scripts, analysis and correlation of events in logs, penetration tests, • knowledge of the ITIL and Prince 2 methodology at the Foundation level - an additional advantage will be the possession of certificates, • experience in team management, • the ability of analytical and business thinking, • ability to solve problems, • ability to work in a team and under time pressure, • availability, • Driving license. B.
(Cybersecurity Operations) Lead Analyst / HSBC Service Delivery (Polska) Sp. z o.o.	• Supporting cyber security incidents through to eradication and feed in to the Post Incident Review process that delivers detailed analysis on the root cause of incidents investigated and produces findings and recommendations that support control adjustments to better protect the	• 5+ years of experience in cyber security senior analyst role or similar. • Formal education and advanced degree in Information Security, Cyber-security, Computer Science or similar and/or commensurate demonstrated work experience in the same. • Technical expertise in analysing threat event data, evaluating malicious activity, documenting unusual files and data and

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.

	bank. • Communicating new use cases (go-live, demise, tuning), to the cybersecurity operations teams, supporting the Cybersecurity Operations Manager in ensuring all teams are prepared to take on the additional workload and have sufficient tools, training and capability to do so effectively. • Researching emerging threats and vulnerabilities to aid in the identification of cyber incidents. • Applying structured analytical methodologies to maximise threat intelligence growth and service efficacy. • Train, develop, mentor and inspire cybersecurity colleagues in area(s) of specialism. • Collaborate with the wider Cybersecurity (and IT) teams to ensure that the core, underlying technological capabilities that underpin an effective and efficient operational response to current and anticipated threats and trends remain fit for purpose.	identifying tactics, techniques and procedures used by attackers. • Expert level knowledge and demonstrated experience in analysis and dissection of advanced attacker tactics, techniques and procedures in order to inform adjustments to the control plane. • Expert level of knowledge and demonstrated experience of common log management suites, Security Information and Event Management (SIEM) tools, use of "Big Data" and Cloud-based solution for the collection and real-time analysis of security information. • Detailed knowledge and demonstrated experience of common cybersecurity technologies such as; IDS / IPS / HIPS, Advanced Anti-malware prevention and analysis, Firewalls, Proxies, MSS, etc. • Good knowledge of key information risk management and security related standards including OWASP, ISO2700x series, PCI DSS, GLBA, EU data security and privacy acts, FFIEC guidelines and NIST standards. • Functional knowledge of scripting, programming and/or development of bespoke tooling or solutions to solve unique problems. • Functional knowledge and technical experience of 3rd party cloud computing platforms such as AWS, Azure and Google. • Basic knowledge and demonstrated experience in common cybersecurity incident response and forensic investigation tools such as: EnCase, FTK, Sleuthkit, Kali Linux, IDA Pro, etc. • Ability to speak, read and write in English, in addition to your local language.

3.2. Overview of job offers in the field of Data Protection

Job offer / enterprise	General description	Skills required (professional, social and transversal)
Data Protection Engineer – SAAS / Sii sp. z o.o.	• Delivering security solutions for the SaaS, IaaS, PaaS cloud infrastructures – integration at proxy and/or API level to deliver corporate level of security to third party cloud solution used by business divisions • Design of on-prem/off-prem/could based components of chosen security system • Development stage implementation of chosen technologies • Ensuring that individual security solutions form an effective security system as a whole • Creating detailed solution designs that fit well into bank's established platforms and core eco-systems • Supporting product management and solution architecture in identifying effective solutions • Providing 3rd level engineering support for security products • Designing system-to-system interfaces that meet security requirements	• Graduate degree in Information Technology, Computer Science or related subject • Proven track record of min. 8 years of work experience in IT and 2 years in a similar role (engineering/infrastructure integration) • Overall knowledge on security concepts (data security & application security) • Working knowledge & experience with one or more of the following areas in IT Security: Cloud Enablement, Cloud Access Security Broker (CASB) / Azure security solutions – MS provided / AWS security solutions – Amazon provided / Data Encryption / Data Masking for SaaS solutions / Federation Services. ADFS, PING Federate, etc. / Public Key Infrastructure (Certificate Management, Cryptography) / Data Loss Prevention / Information Rights Management • KMIP, KeyVault experience (nice to have) • Fluent written and spoken English

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.

Junior Data Protection Analyst / CROWE GLOBAL	• Ongoing support for consulting contracts in the field of information security and personal data protection • Support of the Consulting team in administrative work (back-office) • Preparation of documentation regarding information security / personal data protection • Support in mapping the processing of personal data • Support for the e-learning platform • Ongoing tracking of changes in regulations	• Very good command of English (B2 level) • Practical knowledge of MS Excel • Very good organization of work, responsibility and independence • Ease in establishing and maintaining interpersonal contacts • Experience in running projects is welcome
Data Security Specialist / Accenture Technology	• Development of processes supporting the protection of sensitive data at clients • Implementing technological solutions in the area of data protection related to masking, categorization, data detection and encryption • Designing and implementing platforms to prevent data leaks in complex environments • Support for the GDPR implementation process	• Knowledge of issues Privacy, Data Masking, Test Data Management • Experience with Public Cloud Providers AWS and / or, b> Azure • The advantage will be knowledge and experience in working with IT security solutions, for example: Delphix, Informatica, Symantec • Experience in projects related to ICT security is welcome • Certificates in the field of IT security, project management or product certificates will be an additional advantage • Very good command of English (especially the ability to read documentation and communicate with other members of the project team) • Very good knowledge of the Polish language
Date Protection	• Ongoing cooperation with Date Protection	• Fluent English C1 / C2, welcome "british english";

Specialist / Spring Professional Poland	Office; • Region support (8 European countries); • Collaboration with the headquarters located in the UK; • Cooperation with employees from various business lines; • Implementation of new procedures and regulations; • Practical and substantive support of co-workers.	• Higher legal advocacy; • A legal counsel's app is welcome; • Practical and material knowledge of RODO / GDPR regulations; • Big self-reliance and a sense of duty; • Willingness to act in an international work environment.
Data Protection Inspector / TAURON Dystrybucja Pomiary sp. z o.o.	• Monitoring compliance with the provisions on the protection of personal data and the Personal Data Protection Policy in the Company • Designing and implementing activities aimed at raising the awareness of all employees of the Company in the field of personal data protection • Conducting regular audits of compliance with the law processing of personal data in the Company and audits of entities entrusted with the processing of personal data by the Company • Participating in the design of new solutions and products, including reviewing proposed legal, technical or organizational solutions in order to maintain the compliance of the Company with the provisions on the protection of personal data	• Min. 3 years of experience related to fulfilling the function related to the protection of personal data • Driving license. B • Knowledge of applicable European and national regulations on the protection of personal data • Building partnerships, proposing improvements, striving for results, making decisions, constantly improving • Higher education in law, IT or in the field of new technologies • Experience in conducting trainings • Ability to plan and carry out audits • Knowledge of the functioning of the information security management system in the meaning of ISO 270xx standards • Practical knowledge of the risk assessment principles for the processing of personal data or the scope of measures securing personal data

	• Supervising the keeping of records related to the protection of personal data to which the Company is obliged under the provisions on the protection of personal data and the Personal Data Protection Policy and making their ongoing reviews in terms of current and correctness • Informing the administrator (Company) and employees of the obligations incumbent upon them under the law on the protection of personal data and advise them in this matter • Providing on-request recommendations for the assessment of the effects on data protection and monitoring their implementation in accordance with art. 35 RODO and applicable process instructions • Cooperation with the supervisory body and acting as a contact point for the supervisory body on all matters related to the processing of personal data, including in relation to previous consultations regarding the impact assessment on personal data protection • Taking necessary actions in the event of incidents of personal data breach in accordance with the provisions on the protection of personal data • Preparation and updating of internal regulations regarding the protection of personal data in force at the Company	

	• Giving the administrator (the Company) ongoing support in the design and implementation of appropriate organizational and technical measures ensuring the protection of personal data at an adequate level • Supporting the employees of the Company in the performance of duties under the provisions on the protection of personal data, in particular when designing and modifying the consent clauses and information clauses • Preparing an annual report on the status of personal data protection in the Company for the Management Board of the Company • Participation in processes and procedures regarding the protection of personal data, in accordance with the Personal Data Protection Policy and appropriate instructions regarding processes	
Senior Data Security Specialist / T-mobile	• Participation in data processing projects as a consultant • Implementation of mechanisms supporting data protection in the organization • Conducting audits and monitoring the application of data security procedures in the organization • Cooperation with a cell responsible for technological security (IT Security) • Conducting training and information	• Very good knowledge of the technical aspects of data protection • Knowledge of regulations regarding the protection of personal data and information security rules • Higher education or during studies (preferred courses: IT, telecommunications) • Three years of experience in the area of personal data protection or information security • Knowledge of tools to prevent data leakage

	campaigns on data security • Preparation and updating of data processing documentation	• Very good knowledge of English • Knowledge of the security aspects of IT systems will be an advantage
Data Security Specialist / DINO Supermarket	• Support for the Information Security Administrator in the scope of activities provided for in the Act on the Protection of Personal Data • Reviewing contracts and procedures for information processing • Testing processes for ensuring safety • Participation in projects regarding the processing of personal data and adaptation of the Company to the GDPR • ABI support in current projects • Development of in-house procedures related to personal data processing policy and responsibility for their implementation • Conducting training in the field of data security	• Higher education, preferred law or administration • Experience in a large organization with a structured structure • Basic knowledge of personal data protection regulations • Basic knowledge of standards in the area of information security • Experience in independent project management • Interpersonal skills

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

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.

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 labor 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 labor market institutions. Pursuant to the Act on the promotion of employment and labor 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 certificates for which a system for validation and certification of learning outcomes at the international level has already been developed.

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.

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).

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. Other important issues regarding the topic of the report

The Polish IT market occupies an important place on the European IT market. It is estimated that the domestic software and IT services market is the second (after Russia) market in Central and Eastern Europe. Its growth in recent years has been at 7.2% per year. The main growth drivers of the IT market in Poland include: inflow of foreign investments, availability of public aid and new directions of the sector's development. The largest global ICT concerns are present in Poland, such as Microsoft, HP, Google, Oracle, IBM, and SAP. In general, employers on the IT market are looking for employees with high technical qualifications, often certified by various types of certificates.

A successful organization should have the following multiple layers of security in place to protect its operations:

- Physical security, to protect physical items, objects, or areas from unauthorized access
- and misuse;
- Personnel security, to protect the individual or group of individuals who are authorized to access the organization and its operations;
- Operations security, to protect the details of a particular operation or series of activities;
- Communications security, to protect communications media, technology, and content;
- Network security, to protect networking components, connections, and contents;
- Information security, to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology.

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.

6. Executive Summary and Resume

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 organisations 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 unauthorised 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 risk.

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.

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.