MYKOLAS ROMERIS UNIVERSITY


# Desk Research Lithuania

| | |
|---|---|
| **Document Details:** | |
| Reference | **TeBeISi** |
| IO / Activity | IO1 – Desk research |
| Author(s) | Irena Zemaitaityte Agata Katkoniene, Odeta Merfeldaite, Asta Railiene |
| Character | Country Report Lithuania |
| Date | 15.12.2018 |

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.

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



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)

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 Organisations

A new reading of the Law on Legal Protection of Personal Data of the Republic of Lithuania was adopted 16 July 2018. The purpose of this law is to protect the fundamental rights and freedoms of people, in particular the right to the protection of personal data, and to ensure a high level of protection of personal data. Article 3 of the Law, points (2) and (3) state that it is forbidden to publicly disclose the personal code and to process the personal code for direct marketing purposes. Art. 5 defines peculiarities of personal data processing in work-related cases 1 p. 'It is forbidden to process data on convictions and criminal offenses of a candidate for employment or work, and personal data of a person, except where such personal data are necessary to verify that the person complies with the requirements for the performance of duties or work functions as defined in statutory and implementing legal acts"; 3 p. "When processing video and / or audio data in the workplace and in the premises of the controller of such data or in the areas where the controlled employees work, personal data relating to the monitoring of the behavior, location or movement of employees shall be notified to such staff upon signature of informing of such processing or other means of proving the fact of informing '. This law also defines the supervisory authorities, the provisions of these institutions on infringement proceedings, and the procedure for imposing administrative fines.

31 October 2018 Guidelines for Implementing Appropriate Organizational and Technical Data Security Measures for Personal Data Controllers and Managers were adopted; the document provides that the basic personal data security tool for the organization's personnel having access to personal data is clearly defined and documented responsibilities and roles, as well as competencies in dealing with personal data. The organization shall have a register of IT resources used for the processing of personal data (hardware, software and network equipment). The register shall contain at least the following information: type of IT resources (e.g. server, workstation), location (physical or electronic). Managing the registry must be assigned to a specific person, such as an IT specialist. The document states that the organization must establish the basic procedures to be followed in the event of an incident or personal data breach, in order to ensure the continuity and availability of personal data processing in IT systems.

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

2 July 2018 a recommendation on procedures for identifying, investigating, reporting and documenting personal data breaches was adopted. Also in Lithuania there function and are in force other previously adopted legal acts and recommendations related to personal data protection: Recommendation on Records of Data Processing Activities, Related to the Protection of Personal Data: Recommendation on Records of

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 Processing Activities (2018); Guidelines for Ensuring the Security of Personal Data Processed in Healthcare Facilities (2017); Recommendation On the Protection of Personal Data and Privacy in the Use of Wireless Networks (2017); Recommendation On Protection of Personal Data on Android Devices" (2015); Recommendation On the Use of Cookies and Similar Devices (2011) and other legal acts[1]

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

In Lithuania, there is a wide range of training (1.5 hours to several days) on data and information security. Most often training is provided by private institutions, for example: Cyber Security Academy founded by UAB "Hermitage Solutions"[2] that ai mis to train IT specialist who is able to solve complicated cyber security issues in a timely and efficient manner and to assess the vulnerability of his organisation's IT infrastructure. UAB "Atea"[3] that is the leading Baltic supplier of IT solutions and services and assist customers with specialist competences, products, services and solutions within IT infrastructure, software development and security. NRD Cyber Security [4] that is a cybersecurity technology consulting, incident response and applied research company. The company focuses on services for specialized public service providers (law enforcement, national CERTs, telecoms, national communication regulators, national critical infrastructure), the finance industry and corporations with high data sensitivity. UAB "Competence Development"[5], taht offer training courses to prepare for the most popular certifications, which are the basis for work with other manufacturers' equipment, so these certifications are often preferred by employers not only in Lithuania but also abroad.

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

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

[1] https://www.ada.lt/go.php/lit/Valstybines-duomenu-apsaugos-inspekcijos-rekomendacijos/2
[2] www.cybersecurityacademy.lt
[3] www.atea.lt
[4] www.nrdcs.lt
[5] www.kompetenc.lt

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.

GDPR violations”; "Protection of personal data and violations of personal data legislation in 2018";

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

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.

## 3.1. 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 |
|---|---|---|---|---|
| Information security training | Main content: Data security and data deletion; Social engineering; E-mail, phishing and communicatin programs; Viruses and Malware; Passwords and authentication; Physical security; Security outside office and public Wi-fi networks; Hackers; Internet browsing; Cloud computing services; Mobile safety; Social networks | basic | Social/ professional | https://www.atea.lt/paslaugos/mokymai/informacijos-saugos-mokymai/ |
| Cyber security training | The aim is to raise awareness of cyber security threats and the most common attacks. Focuses on:<br>• Legal aspects of information security;<br>• Information Security Standards (ISO / IEC);<br>• Common principles for safe online work;<br>• Technical aspects of cyber security;<br>• IT governance and leadership techniques in COBIT 5;<br>• Implementation of Information Security Management System (according to ISO / IEC 27000 standards). | basic, intermediate / proficient user | Professional, social and transversal | https://www.nrdcs.lt/lt/Paslaugos/mokymai-/7 |
| Information security training for non professionals | Training content:<br>• Safe work in the local environment<br>• Secure work on local computer network and with mobile media<br>• Safe use of the Internet<br>• Secure remote access to company information<br>• Response actions in the event of an incident | basic, intermediate / proficient user | Professional, social and transversal | http://www.kompetenc.lt/Inf.aps.mok.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.

| | | | | |
|---|---|---|---|---|
| Basics of cyber security | The core of cyber security basics is to get to know the current issues of IT security and to prepare for practical cyber attacks. | proficient user (IT professional) | Professional | https://www.cybersecurityacademy.lt/bazinis-kibernetinio-saugumo-kursas |
| Hack IT to Defend IT (L1) | The main focus is on network vulnerabilities, in-depth analysis of critical areas. Training content: ethical invasion and basics of protection; Testing methods for testing your systems; How vulnerabilities are discovered and exploited; Fundamentals of Social Engineering; Types of protection against different types of attacks | proficient user (IT professional) | Professional | https://www.cybersecurityacademy.lt/hack-it-to-defend-it |
| Hack IT to Defend IT (L2): web applications | The aim of the training is to demonstrate the most common security issues of web applications and how they can be exploited for cyber attacks | proficient user (IT professional) | Professional | https://www.cybersecurityacademy.lt/hack-it-to-defend-it-l2-web-apps |
| Ethical hacker practitioneer (L3) | The training analyzes how to force applications to do what for they haven't created. | proficient user (IT professional) | Professional | https://www.cybersecurityacademy.lt/etinis-hakeris-praktikas-l3 |
| Safe programming | The training focuses on web application vulnerabilities, how to identify and remove them, thus ensuring the security of web applications in their development phase. | proficient user (IT professional) | Professional | https://www.cybersecurityacademy.lt/saugus-programavimas |
| IT security practitioneer | The course provides an in-depth overview of all aspects of IT security and the latest security trends and technologies | proficient user (IT professional) | Professional | https://www.cybersecurityacademy.lt/it-saugumo-praktikas |
| Information security practitioneer | Trainings analyze latest security technologies and trends, risk assessment and management and other cyber security factors | proficient user (IT professional) | Professional | https://www.cybersecurityacademy.lt/informacijos-saugumo-praktikas |

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.

| | | | | |
|---|---|---|---|---|
| Cyber security incident management | These courses teach you how to effectively manage various cyber attacks within your organization. During training, IT specialists understand how incident management is going, how to collect information, analyze and evaluate areas that need to be addressed first after an incident | proficient user (IT professional) | Professional | https://www.cybersecurityacademy.lt/saugumo-incidenu-valdymas |
| IT securty awarness training | The training discusses the risks and causes of IT security. There are also discussions about strategies used by criminals to extract data and social engineering methods. | proficient user (IT professional) | Professional | https://www.cybersecurityacademy.lt/it-saugumo-mokymai-darbuotojams |

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.

## 3.2. 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 |
|---|---|---|---|---|
| Protection of personal data: GDPR requiriments training | Training content: Basic principles and categories for the protection of personal data. Duties of data protection specialists and their implementation. Rights of data subjects and their adequate assurance. Responsibility for non-compliance with legal protection requirements for personal data. The Company's Local Legislation in the Field of Legal Protection of Personal Data. Evaluation of Impact on Data Protection. | proficient user | Professional | https://renginiai.kasvyksta.lt/56766/asmens-duomenu-apsauga-bdar-reikalavimu-mokymai |
| Protection of personal data and responsability of GDPR violations | Training content: Concept of personal data protection, principles of processing; Legal requirements for the | Basic /intermediate / proficiant user | | http://www.auditorija.lt/mokymai-kursai/9577-asmens-duomenu-apsauga-bei-atsakomybe-uz-asmens-duomenu-teises- |

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.

| | | | | |
|---|---|---|---|---|
| | processing of personal data; General remarks on the implementation of personal data protection | | | aktu-pazeidimus-isigaliojus-es-bendrajam-duomenu-apsaugos-reglamentui-bdar |
| Protection of personal data and violations of personal data legislation in 2018 | Training content: Personal data protection legislation; Rights and obligations of the controller; Persons whose data are managed by rights and duties; What can and cannot be done by debt collectors, utilities, etc., the limits of their responsibilities, the most common mistakes. Explanations from the Personal Data Protection Inspectorate; Employees, their stored data and employers' rights; Video cameras at work and other public places to know; Case law and interpretations in the field of personal data protection | basic | Social/ professional | http://www.auditorija.lt/mokymai-kursai/9220-asmens-duomenu-apsauga-bei-atsakomybe-uz-asmens-duomenu-teises-aktu-pazeidimus-2018-m |
| GDPR | Training content: GDPR concepts and fields of application; Regulation, sanctions and fines; Data Protection Officer, Function, | basic | Social/ professional | https://www.sabelija.lt/lt/paslaugos/435-seminaras-bendrasis-duomenu-apsaugos-reglamentas |

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.

| | | | | |
|---|---|---|---|---|
| | Need; Data processing by means of systems; IT tools and commitments; Preparing for data processing and storage under GDPR | | | |

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

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

11-26 July 2016 public opinion and market research company „Spinter Tyrimai" on behalf of the Human Rights Monitoring Institute, conducted a survey of business entities operating in Lithuania on data protection in Lithuania. The survey was carried out throughout Lithuania and was attended by representatives of 50 companies operating in Lithuania. Respondents were selected using the quota selection method, applying business type quota: startups - telecommunication and financial companies – and others, respectively 60 - 20 - 20. It appeared that businesses surveyed believe that the current legal regulation of data protection in Lithuania is sufficient. Most believe that the legal regulation of Lithuania is sufficient, there are telecommunication and financial services companies (80%), the least - among other companies (60%). At present, telecom and financial services companies are among the most supervised, so they can best express their attitude towards the existing regulatory regime as well. Almost half of the respondents (48%) did not have the opinion whether the penalties provided for in Lithuanian legislation for violations of data protection requirements were sufficient at the moment. The other half (46 percent) believed that the punishment was sufficient, and the minority consider the punishment insufficient. As mentioned above, penalties for violations of data protection requirements in Lithuania were among the lowest in the EU, but they were applied relatively frequently and for minor violations (e.g. non-registration as a data controller - an obligation that is generally repealed by the General Data Protection Regulation). Most of those who did not know about punishment were among other companies (70%), and most of those who thought that punishment was sufficient - among startups (53.3%). 55.6 percent companies that did not register as personal data controllers did not have an opinion or did not know about penalties for violations of data protection requirements, the number of such respondents among registered companies was 28.6%. These results could be explained by the fact that registering as a personal data controller is one of the main administrative and bureaucratic duties of personal data controllers in accordance with the Law on Legal Protection of Personal Data of the Republic of Lithuania. Compulsory instructions and sanctions of the State Data Protection Inspectorate (further SDA) are often imposed for non-compliance. As a result, companies that have registered as personal data controllers are more likely to face possible sanctions for violations of legal protection of personal data. The encouraging result is that the majority (74%) of the survey participants trust the institutions responsible for the supervision of privacy and personal data protection in Lithuania: 12%. fully trusted, 62 percent are more likely to trust. Most companies trusting Lithuanian institutions are among telecom and financial services companies: even 80 percent. replied that they are more likely to trust the

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.

Lithuanian authorities; however, there was no single response amongst them that they had full confidence in the institutions. Most of the companies surveyed (even 72 percent) currently attach great importance to data protection. Most often, companies solve personal data protection problems with internal resources: the majority of respondents say that these problems are solved by a staff / administration employee (86%), 44%. - IT employee, 40% has a dedicated employee who takes care of data protection. Very few companies apply for assistance to external specialists - data protection specialists (6%), IT service providers (4%) or lawyers (2%). In all telecom and financial services companies (100%), data protection issues are solved by personnel / administration staff as well as by 50%. these companies have a dedicated employee and 40 percent these problems are solved by IT staff. These companies do not seek help from outside specialists. The situation among startups and other companies is similar, only among these companies there are several respondents who apply for help from external specialists. One company said that it is not solving data protection issues, and no such companies have emerged among startups and telecom and financial services companies.

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

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

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

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) |
|---|---|---|
| UAB "LIDL LIETUVA" https://www.cvbankas.lt/informacijos-saugumo-specialistas-e-vilniuje/1-5631133 | INFORMATION SECURITY SPECIALIST job description:<br>Organize and control the implementation of information security policy;<br>Analysis, management and prevention of information security risks;<br>Control and assurance of compliance with information management and security;<br>Training and consultancy on IT security for company employees;<br>Coordination and solutions for information security incidents;<br>Prepare reports | REQUIREMENTS:<br>Higher university education;<br>At least 2 years of experience in information security management;<br>Experience in analyzing IT incidents, information from monitoring tools and audits;<br>Ability to work independently;<br>Communicability, initiative, analytical thinking;<br>Good English skills, German is an advantage |
| STATE ENTERPRISE AGRICULTURAL INFORMATION AND RURAL BUSINESS CENTRE [LT.: VALSTYBĖS ĮMONĖ ŽEMĖS ŪKIO INFORMACIJOS IR KAIMO VERSLO CENTRAS (ŽŪIKVC)] http://www.vic.lt/struktura_ir_kontaktai/informacijos-saugos-specialistas/ | INFORMATION SECURITY SPECIALIST:<br>coordinate and control the implementation and compliance with the requirements of the Republic of Lithuania legal acts regulating information security;<br>• prepare the results of information resource compliance assessment and risk assessment and submit them to the State Information Resource Compliance Monitoring System (ARSIS);<br>• organizes and conducts an annual and extraordinary (if necessary) risk assessment, administers the electronic Risk Management Register;<br>• Analyzes, analyzes and solves information security events, incidents and cyber incidents, administers electronic event and incident logs;<br>• Performs an annual classification of information;<br>• Initiates and conducts business continuity plans and recovery plans testing; | REQUIREMENTS:<br>Higher university education;<br>At least 2 years of experience in information security management;<br>Experience in analyzing IT incidents, information from monitoring tools and audits;<br>Ability to work independently;<br>Communicability, initiative, analytical thinking;<br>Good English skills |

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.

| | | |
|---|---|---|
| | • Performs periodic user access checks;<br>• participates in the management of ongoing projects: develops information security and cyber security requirements for the IS and registry specifications administered by the center and coordinates daily tasks in the Change and Defect Management System;<br>• organizes and performs conformity assessment of information center security requirements;<br>• organizes and implements information security and cyber security awareness training for center staff and external information resource users, prepares training and sharing material for users;<br>• performs the functions of the Information Systems and Registers Security Officer administered by the Center in the IS and Registry Data Security Regulations administered by the Center and in other legal acts of the Republic of Lithuania;<br>• co-ordinates and controls the implementation and enforcement of legal requirements of the Republic of Lithuania regulating cyber security;<br>• carries out the functions of a cyber security manager;<br>• Coordinates and controls the implementation and compliance with the requirements of the Information Security Management System in accordance with the requirements of ISO / IEC 27001: 2013:<br>• ensure the protection of personal data in information resources within their competence;<br>• Conduct measurements of the effectiveness of organizational and technical measures for Information Security Management System, information security, cyber security, and personal data protection, presented by the management during the assessment meeting;<br>• represent other institutions, bodies, companies and organizations in matters of information security, cyber security and competence in the field of personal data protection. | |
| CVMARKET.LT CLIENT<br>https://www.cvmarket.lt/informacijos-saugumo-specialistas- | INFORMATION SECURITY SPECIALIST:<br>• Coordinate the implementation of international security directives and standards | REQUIREMENTS<br>• University education<br>• 2+ years of experience with Information Security |

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-officer-vilnius-alliance-for-recruitment-329904 | • Coordinate and conduct internal audits and system security needs analysis, to provide conclusions<br>• Conduct information security training within the company<br>• Develop national contingency concepts for information security incidents<br>• Coordinate and control the implementation of measures arising from operational information security events (IS incidents)<br>• Regularly aggregate common information security indicators and produce related messages (eg implementation status);<br>• Supervise external inspections and audits;<br>• Participate in the continuous development of international information security policies and security directives;<br>• Regular reporting to international information security representative. | • 1+ year experience in project management<br>•Work experience in network or system administration<br>• Communicability, organization, initiative<br>• good knowledge of English |
| „INFOSTRUKTŪRA“ https://www.plius.lt/skelbimai/informacijos-saugos-specialistas-e-3064587.html | INFORMATION SECURITY SPECIALIST:<br>Continuous monitoring of the situation in computer networks;<br>Incident detection, removal;<br>Incident analysis, vulnerability detection and removal;<br>Common assessment of computer network security, audit, implementation of preventive measures. | REQUIREMENTS:<br>Excellent skills for working with Windows, Linux, Unix operating systems;<br>Web programming basics (PHP5, MySQL, JavaScript);<br>Knowledge of solutions and tools for security on computer networks;<br>Computer network administration basics;<br>Good knowledge of English;<br>Analytical thinking, honesty, quick orientation, flexibility, initiative<br>We will give priority to specialists who:<br>Has implemented IT systems security solutions in practice;<br>Has certificates (SCNS, SCNP, CEH); |
| UAB "ALLIANCE RECRUITMENT" | INFORMATION SECURITY SPECIALIST: | REQUIREMENTS<br>Higher education (IT or science); |

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.

| | | |
|---|---|---|
| https://www.cvbankas.lt/informacijos-saugos-specialistas-e-vilniuje/1-5611845 | Enterprise Information Security Management by developing, coordinating and supervising the implementation of a safety management system;<br>Analysis of information security risks, assessment of risk mitigation actions and preparation of risk reduction plans;<br>Preparation of information security policies and other required documentation;<br>Control and assurance of compliance with information management and security;<br>Information security incident resolution / decision coordination;<br>Testing the functionality of system improvements, preparing instructions for new processes and training their key players / training of company employees;<br>Advising company employees on IT security issues. | 2+ years of experience working with / implementing information security management systems across the enterprise;<br>Experience in analyzing IT incidents, information from monitoring tools and audits;<br>Knowledge of the importance of IT management (operating systems, databases, IT networks and infrastructure, IT systems) for information security compliance;<br>Communicability, initiative, perseverance, analytical thinking and ability to work independently;<br>Good knowledge of English and Lithuanian is essential; knowledge of Russian would be an advantage;<br>An information security knowledge certificate (CISA, CISM, CRISC) would be an advantage. |

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.

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

| Job offer / enterprise | General description | Skills required (professional, social and transversal) |
|---|---|---|
| STATE DATA PROTECTION INSPECTORATE [LT.: VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA] https://www.ada.lt/go.php/lit/Valstybine-duomenu-apsaugos-inspekcija-skelbia-konkursa-i-prieziuros-skyriaus-patarejo-pareigas | MAIN SPECIALIST OF THE SUPERVISORY OFFICE.<br>Function Level - A, Job Category - 13.<br><br>FIELD OF ACTIVITY:<br>A civil servant acting in this capacity carries out functions in the sphere of general activity - law, international relations, as well as in the field of special activities - in the field of personal data protection and international cooperation | SPECIAL REQUIREMENTS:<br>University degree (undergraduate and postgraduate degree) or equivalent university degree in law;<br>Have at least 3 years of legal work experience;<br>Pay a foreign language (English, French or German) at advanced user level B1;<br>Be familiar with the Constitution of the Republic of Lithuania, laws of the Republic of Lithuania, resolutions of the Government of the Republic of Lithuania and other legal acts regulating public service, public administration, data protection, preparation of documents, management and accounting and drafting of legal acts, as well as European Union and international legal acts and to be able to apply them in practice;<br>Ability to work with a computer in MS Office software package;<br>Be able to manage, systematize, analyze, summarize information and draw conclusions;<br>Fluent writing and oral presentation skills;<br>To be able to plan and organize the activities of the department. |

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.

| | | |
|---|---|---|
| UAB "BALTIC GROUND SERVICES"<br>https://www.cvbankas.lt/teisininkas-duomenu-apsaugos-specialistas-vilniuje/1-5276555 | Lawyer - DATA PROTECTION SPECIALISTFIELD OF ACTIVITY:<br>Ensure implementation of data protection requirements within the company;<br>To perform the functions of the Data Protection Officer;<br>Implement and control compliance with data protection principles and requirements within the company;<br>Analyze, evaluate, organize documents, processes related to data processing, data provision to third parties and others;<br>Advise and train the company's employees on data protection, company compliance issues;<br>Promote a data protection culture in the company. | REQUIREMENTS:<br>University degree in law;<br>Knowledge of legal acts of the Republic of Lithuania and the European Union regulating the protection of personal data;<br>Ability to manage data processing processes;<br>Experience in working with personal data protection (at least one year);<br>Expert knowledge of data protection rights and practices;<br>Ability to summarize information and draw conclusions in a clear and precise manner in written and oral form;<br>Ability to independently plan and organize your work, make proposals and make decisions;<br>Excellent business communication skills, work ethics knowledge;<br>Very good oral and written knowledge of English and Russian;<br>Excellent computer skills. |
| CVMARKET.LT CLIENT<br>https://www.cvmarket.lt/duomenu-apsaugos-pareigunas-vilnius-turto-bankas-vi-332275 | DATA PROTECTION OFFICER<br>Job description<br>Practical application of the General Data Protection Regulation (GDPR) (lt. BDAR) requirements in SE Turto bankas;<br>Control of compliance with the Law on Legal Protection of Personal Data, GDPR and Internal Processing of Personal Data at SE Turto bankas;<br>Communication with data protection authorities;<br>Employee information and consultancy, organization of training relating to data protection;<br>Management of data protection risks and implementation of necessary changes in the company; | REQUIREMENTS:<br>University or equivalent education in social sciences;<br>Excellent knowledge of the legal acts of the Republic of Lithuania and the European Union regulating personal data protection and practical experience;<br>Experience in implementing data protection policies and legislation;<br>Good skills in working with MS Office programs;<br>Driver's licence (B category); |

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.

| | | |
|---|---|---|
| | Constant update of data protection policies and legislation. | Knowledge of English (Level B2). |
| LITHUANIAN RADIO AND TELEVISION CENTRE (TELECENTRE) [LT.: LIETUVOS RADIJO IR TELEVIZIJOS CENTRAS (TELECENTRAS)] http://www.telecentras.lt/wp-content/uploads/2017/12/DUOMEN%C5%B2-APSAUGOS-PAREIG%C5%AANAS.pdf | DATA PROTECTION OFFICER<br>Job type:<br>Managing a project in preparation for the practical application of GDPR requirements in the organization;<br>Continuous monitoring of compliance with data protection law and GDPR as well as internal policies for the processing of personal data;<br>Communication with data protection authorities;<br>Employee awareness raising through internal communication channels and periodic training of relevant personnel;<br>Managing identified risks in the area of data protection and implementing the required changes on an organizational scale;<br>Development and ongoing updating of data protection policies and procedures;<br>Investigation and preparation of complaints from any EU data protection supervisory authority. | REQUIREMENTS:<br>Excellent knowledge of personal data protection legislation and experience of practical application and understanding of GDPR;<br>Experience in implementing data protection policies, procedures and training materials;<br>Internal and external stakeholder consultation on data protection issues;<br>Ability to work independently as well as to communicate smoothly and constructively with different people profiles in the organization. |

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 aquired outside formal Education

In order to support the practical work of Data Protection Officers, which, under the EU General Data Protection Regulation, have been in place since 25 May 2018, it is imperative to have a large number of companies and all state agencies to attend special theoretical and practical training. One of the key roles of the officer is to help monitor how the GDPR is being complied with within the company. For this purpose, the official may collect information, verify that the data processing activities meet the requirements, advise the controller or the processor, and make recommendations to him. Training of Data Protection Officers in Lithuania is being organized in accordance with the accredited PECB program. PECB is accredited according to ISO / IEC 17021, 17024, 17065 standards, and is accredited by international organizations IAS (International Accreditation Service), IAAR (The Independent Association of Accredited Registers), IPC (The International Personnell Certification Association). The training material is provided and the exam takes place in English. Usually such training is offered by private training institutions. The Data Protection Certificate is one way of demonstrating to both the employer, data subjects and the data supervisory authority that the Data Protection Officer has specific knowledge. DPC certificates are issued by national and international institutions such as associations of data protection professionals, universities, training institutes for civil servants, etc. One of these centers is located in Vilnius - CTG testing center. Certificates are usually issued after a training course and passing the relevant exam.

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

Training for information security manual (CISM) is organized for experienced professionals. The CISM (Certified Infromation Security Manager) program is designed for experienced information security managers, managers, consultants, and employees directly responsible for information security management within the organization. This program is for those who develop, manage, maintain or evaluate information security. This certification shows that the information security specialist has the experience and knowledge to provide the appropriate management and consulting services. CISM defines core competencies and international performance standards to be met by those responsible for information security management. The CISM program is specifically designed for experienced professionals with expertise in information security management. CISM certification is for individuals who have been in charge of or have held similar positions and experience in the following areas for at least three years: combining an information security strategy with operational objectives; identifying and managing information security risk factors for performance targets; managing the information security program; developing and managing an incident and business continuity program. CISM Certified Professionals must: have a five-year (Information Security Manager - three years) experience in Information Security; pass an exam; to meet the annual requirements for further training. The course is based on international practices and standards[6].

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

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

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

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

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

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.