Desk Research ITALY

Document Details:	
Reference	**TeBeISi**
IO / Activity	IO1 – Desk research
Author(s)	Mr Paolo Zaramella, StudioCentroVeneto sas
Character	Country Report ITALY
Date	15.01.2019

Funded by the Erasmus+ Programme of the European Union

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

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

.

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 GDPR - 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

As Italy is a member of the European Union, all national legislation relating to Information Security and Data Protection / Privacy derives from European Regulations and Directives.
In this sense, on May 16, 2018, the Council of Ministers approved the Legislative Decree to implement the NIS (Network and Information Security) Directive in our country.
The Italian government has opted for a "soft" approach, limiting itself for the most part to incorporating into the legislative decree what was already established by Directive NIS 2016/1148 on the security of networks and information systems.
This Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerns measures for a high common level of network and information system security in the European Union.In line with the requirements of Article 7 of the Directive, the transposing decree provides for the adoption of a national cybernetic security strategy by the President of the Council of Ministers.
The strategy should include, in particular, measures for the preparation, response and recovery of services following cyber incidents, the definition of a cyber risk assessment plan and cyber security training and awareness programmes. Most of these elements are already addressed, for the most part, in the current national cybernetic security strategy, outlined in the National Strategic Framework for cybernetic space security of December 2013 and further developed by the National Plan for cybernetic protection and cybersecurity of March 2017. Both documents, in Italian, are attached to this report, as additional and complementary elements to what is reported below.
In summary, the two documents contain the following essential elements:
- The profiles and evolutionary trends of threats and vulnerability/risks of systems and networks, especially those of national interest;
- Tools and procedures to enhance cybernetic capabilities in Italy;
- The roles and tasks of public actors in the field of control;
- The strengthening of organizations and coordination methods at national level between public and private subjects;
- The promotion and diffusion of the culture of information security;
- The operation of the national structures and the connection with the various legislative interventions;
- The realization of protocols and standards of security;
- The development of awareness and communication actions;
- Finally, the implementation of a national "cyber risk management" system.

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

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.

Comparing the Italian legislation with other European realities, it can be affirmed that it is a model halfway between the strongly centralist French one, with a single competent authority, and the decentralised one of the Nordic countries, such as Sweden, where the regulatory and supervisory tasks in matters of cybersecurity are attributed to a series of public agencies competent for specific sectors.
The Security Information Department (DIS) is designated as the single point of contact under Article 8 of the Directive. The DIS will therefore be responsible for liaising with the European Union and coordinating with the cybersecurity authorities in the other Member States.
The current legislation also provides for the establishment within the Presidency of the Council of Ministers of a single "Computer Security Incident Response Team", called the Italian CSIRT, which will replace, merging them, the current National CERT (operating at the Ministry of Economic Development) and CERT-PA (operating at the Agency for Digital Italy).
This merger process could not be easy to manage, which could extend the time for the adoption of the Prime Minister's decree to be adopted later to regulate in detail the organization and operation of the CSIRT.
In any case, the Italian CSIRT will have technical tasks in the prevention and response to computer accidents carried out in cooperation with other European CSIRTs.
The implementing decree reiterates the general safety obligations provided for by the Directive in Article 14. In essence, operators of essential services must adopt technical and organizational measures "adequate" to manage risks and prevent computer accidents.
However, the decree specifies that when adopting such measures, operators must take due account of the guidelines that will be prepared by the Cooperation Group.
These guidelines are therefore of fundamental importance for demonstrating the adequacy of the measures adopted.
The competent NIS authorities may also require the adoption of specific security measures, in consultation with the operators of essential services.
It is therefore likely that operators will soon have more specific guidance on the security measures to be taken, in the form of guidelines or other administrative measures.
Similar security obligations are imposed on digital service providers, who will have to take technical/organisational measures to manage risks and reduce the impact of possible cyber incidents.
The elements to be taken into account by digital service providers for the management of cyber risks are better specified in Commission Implementing Regulation (EU) 2018/151 of 30 January 2018.
The implementing decree specifies that the processing of personal data in application of the decree is carried out in accordance with Legislative Decree no. 196/2003 (Privacy Code).
This reference has become (at least in part) obsolete with the final entry into force of the General Regulation on Data Protection (GDPR) on 25 May 2018, it is to the latter therefore that reference should be made.
Now, in fact, the GDPR is the main regulatory framework regarding the processing of personal data, and has replaced (largely) the former Privacy Code. It would have been appropriate, therefore, to provide for an update of the regulation (also referring to the GDPR) before the final adoption of the decree.
The NIS Directive leaves Member States a margin of discretion as to the type and nature of sanctions applicable, provided that they are effective, proportionate and dissuasive.
In exercising this discretion, the government has decided to establish that the competent authorities will be able to apply administrative sanctions of up to €150,000 in the event of a breach by essential service operators (and digital service providers) of their obligations under the Decree. This is in line with the approach followed by other Member States.
In fact, Germany has provided for sanctions of up to €100,000 for violations of its legislation transposing the NIS Directive, while in the Czech Republic the sanctions rise to around €200,000 (5 million Czech crowns).

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.

After the transposition decree, in force since 26 June, the next steps are to make the provisions of the decree effective and update the National Plan for Cybernetic Protection and 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.

3. Vocational and Continuing Education and Training in this area

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

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

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

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

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

The scenario appears different if we look at the outlook for spending in the future: the highest percentages of increase are expected in mobile and cloud computing, with 63% of companies declaring an increase in expenditure dedicated to the protection of mobile devices (which weighs about 4% of current expenditure) and 59% defining an increasing budget for the protection of cloud computing environments (which currently covers 3% of expenditure). This is followed by security awareness & training (up 56%) and cyber insurance (indicated by 52%, with a current market share of 2.5%).
In the following tables, we summarized 8/10 existing training offers (for Information Security and for Data protection).
As criteria for selection (nowadays, there are thousands of offers at national level) we took in consideration:

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.

- if they are planned also for SMEs and experts;
- mainly proposed by VET providers (and not only from Universities and/or business schools);
- also the geographical position (i.e. North East of Italy);
- with a practical approach (it means: training useful for a skills up-todating).

These three main criteria are applied also in the next chapter (no. 4, about jobs offered in Information Security and for Data protection).

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
1) "Higher training course in Information Security Management"; made by MIP Politecnico in Milan	Understand and evaluate the complexity of security issues that impact on corporate ICT, anticipating them with a proactive approach. Design, evaluate, implement and manage an Information Security Management System integrated with the company's core business, in accordance with the main reference standards, promoting effective management of known or foreseeable risks and anticipating the emergence of new ones. Estimate the costs and benefits of different solutions, evaluate the return on investment in security and understand the organizational implications of Information Security.	High level users: IT experts; cyber security experts; legal experts; ISO (Information Security Officers)	- Underlying technology & hot topics - Organization and management - Legal	Feedbacks from revious students (it is the 14th edition)
2) „Information security" technical course; made by „Il Segno" training school	The course covers the main aspects related to this profession: designing secure computer networks, analyzing existing computer networks trying to identify any weaknesses, intervene in case of virus infections, estimate costs and	Middle level users	Be able to handle technical and regulatory issues of considerable importance, in structures from the smallest to the most complex.	Feedbacks from revious students

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.

	recommend the adoption of particular procedures and software, configure and manage firewalls, encryption programs, hardware components that improve security and much more.			
3) „Information security" basic course; made by ADM Form	The growing use of the Internet and information technologies raises the problem of having to identify the security elements necessary for the performance of the profession, allowing the management of work in an immediate, safe and in full compliance with current regulations, especially with regard to privacy. The aim of the course is to outline the technical, legal and managerial aspects of security and privacy, as well as to provide some basic elements to manage these issues in the most effective way.	basic	be able to understand the Fundamentals of Information Security. be able to understand the Italian privacy law, the provisions of the Privacy Guarantor and the new European regulation. be able to understand the basic elements of telecommunication network security, the advantages of the cloud and security implications. basic knowledge of the ISO/IEC 27001 Information Security Management standard.	Feedbacks from revious students
4) „Information security and Ethical Hacking" middle level course; made	Online course guides students in the field of Information Security. This is one of the largest areas of technology to be covered since every system, network, program needs to be made	The course is addressed to graduates, graduates, technicians and enthusiasts who	- Professions in Information Security - Types of Vulnerability - Kali Linux: The Hacker Operating	Feedbacks from revious students

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.

by Udemy	secure today. That's why companies are always looking for qualified personnel and IT security professionals. This request is answered by Accademia Tomorrow with its online course. It is by following it that you will obtain the information on computer security necessary to become a Professional. With the online course you will be able to become an Ethical Hacker, a professional figure today increasingly widespread that has a very varied and always updated knowledge of computer science.	want to enrich their skills or embark on a career in ICT Security from scratch.	System - Unix, Windows and Network Basics - Passive Discovery - Active Discovery - Sniffing & Password Cracking - Hacker Framework & Useful Resources - Simulation of a computer attack on Windows - Simulation of a computer attack on Linux	
5) „Cybersecurity" course; made by Opificum Foundation	The CYBERSECURITY basic level course has the objective of framing the theme of information security from a regulatory and managerial point of view.	basic	Definitions and Italian context Defense of cybernetic space Regulations The aspects of management and risk management (National Framework of CyberSecurity) Basic technical aspects	Feedbacks from revious students
6) „Master in Cybersecurity";	Digital Transformation is an essential necessity for the continuous development of organizations	The Master responds to the growing demands	• Cyberthreats • Public governance of cybersecurity	Feedbacks from

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.

made by LUISS (business school)	and the country. However, it brings with it great technological, cultural and organisational changes that not only have a daily impact on users, businesses and national and international public administrations. Technological developments such as, for example, IoT, cloud, social, mobile are just some of the emerging issues that all public and private organizations have to deal with. Digital Transformation therefore offers increasing opportunities to companies and organizational structures, which to be seized require the construction of adequate protection systems based not only on technological knowledge, but also on managerial, economic, legal and political knowledge and skills. In fact, in addition to the traditional threats coming from cyberspace, new, increasingly targeted, social and persistent methods of attack are being added.	of the labor market in the public and private sectors of professional profiles specializing in cybersecurity that, in addition to an adequate knowledge of digital technologies, combine managerial, legal and economic skills.	• Italian policies and institutions • European and international policies and institutions • Cybercrime • Digital Forensics • Digital Privacy • Regulation and Contract in Cybergovernance • Enterprise cyberthreats • Enterprise governance of cybersecurity • Risk Management • Economics of Cybersecurity • IT essentials • Introduction to cybersecurity • Networking essentials • Cybersecurity essentials	revious students
7) „Information security" course; made by ESAC Vicenza	The primary objective of the course is to illustrate some important aspects to protect corporate privacy, taking into account the company's computerized management that	Basic; It is addressed to all workers and to all those who want to deepen this issue.	security policy Creation of robust passwords Defend yourself from social	Feedbacks from revious students

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.

	increasingly concerns customer and supplier files, price lists and procedures.		engineering	
8) „Information security" course; made by MAC Formazione Padova	The course Computer Security was born with the main objective of training an expert in cyber security able to create and monitor the right procedures to follow to avoid compromising sensitive data and / or blocking the daily work activities.	Basic; The objective of the course Computer Security in Padua is to transmit you the skills necessary to avoid computer attacks ensuring the necessary computer security of your company.	Email Security: Spam, Phishing, Malware, Cryptolocker etc... Web Security: secure surfing, browser searches, bank fraud, etc... Browser Security: which to choose, the plugin etc.. Passwords: definition of a password, unsafe passwords etc... Antivirus: which to choose and how to configure it Data backup and network protocols Remote access	No
9) „Information security in the companies" course; made by Dgroove Verona	Training course on Corporate Information Security This course allows you to train experienced professionals, even with previous skills and significant seniority in information technology, sensitive and competent on issues of information security.	Middle level	Core business, operational and strategic activities for the company Processes and procedures: daily work activity IT, mobile and other technologies: how everyday depends on them	Feedbacks from revious students

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 introduction course to cybersecurity aims to train experienced professionals, even with previous skills and significant seniority in the field of information technology, sensitive and competent on issues of information security. The technical expert in information security is the one who, knowing the areas and reasons with which computer attacks occur, is able to implement the appropriate defensive strategies for his company. The analysis of the reasons for an attack is particularly important because it allows you to pick up warnings or interpret technical anomalies that would otherwise go unnoticed or almost unnoticed.		Integrated holistic view: examples of cross-dependencies The role of people with respect to technologies Objectives of an attack The layered or onion safety model Direct Attack Use of systems as a bridge The role of viruses Stealing data (or money) Stealing electronic identities The denial of service and the cyber-return Who are the attackers	

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 Data Protection

Name of Training Course	Main Content / Objective	Target Groups (basic /intermediate / proficiant user)	Skills acquired (professional, social and transversal)	Kind of Testimonial
1) „Data Protection Officer" course; made by ASSO DPO	The DATA PROTECTION OFFICER Advanced Specialization Course is aimed at training consultants and privacy representatives of companies in the public and private sector who intend to specialize in accordance with international standards of ISO standards, and in the future hold the role of "Data Protection Officer" or "Data Protection Officer". This new figure has taken on particular importance in the light of the approval of the European Regulation on data protection that unifies the Privacy legislation in the 27 EU member states. The role of the DPO may be covered by both internal employees and external consultants through a service contract.	Privacy contact persons (employees or consultants) who deal with the implementation of the Privacy Policy in companies; Data Protection Officers, Freelancers, Business Consultants, Compliance Officers, Corporate Law.	Several modules, that cover almost all the requested market competences	Feedbacks from revious students
2) „Data Protection	The European Privacy Regulation expressly provides for the obligation for companies and public	Public Administration (PA) Healthcare and Social-	At the end of the specialized privacy training, your Data Protection Officer	No

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.

Officer" course; made by EUCS	administrations to have their Data Protection Manager attend a periodic Privacy Officer Course in order to allow him to maintain his specialist knowledge in the field of privacy. For this reason, EUCS has created a Data Protection Officer Privacy Course, updated to Legislative Decree 101/18, which allows you to acquire and maintain the specific skills to cover the role of DPO in the company and allows you to obtain the International Certification of Data Protection Officer. The Data Protection Manager Course is Certified and Personalized and can be done directly at your company's headquarters or attended in e-learning mode. At the end of the specialized privacy training, your Data Protection Officer will have the legal, organizational and technological knowledge necessary to properly cover the role of Data Protection Officer.	Assistance Financial, Banking and Insurance School and Educational Professionals (lawyers, accountants, labour consultants and notaries) Information Technology, Web and Telecommunications Trade, Distribution and Marketing Tourism and Catering Transport and Logistics Real Estate and Construction Production	will have the legal, organizational and technological knowledge necessary to properly fulfill the role of Data Protection Officer. The DPO course consists of a general module lasting a total of 32 hours and a series of advanced modules lasting 8 hours for each area of specialization chosen.	
3) „Specialist training course for	The main objective of the advanced training course for Data Protection Officers is to provide participants with the general knowledge and skills required to	For experts	Legal information technology	Feedbacks from revious students

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.

DPO"; made by Pegaso (on line University)	perform the role of Data Protection Officer (DPO) or Data Protection Officer (DPO), as required by EU Regulation 2016/679. The DPO is designated on the basis of professional qualities, in particular specialist knowledge of data protection legislation and practices, and the ability to perform its tasks. This figure, of a high professional level, may be an employee of the data controller or of the data controller or fulfil his duties on the basis of a service contract and therefore may be a freelancer.		Administrative law European Union law Business Economics	
4) „On line Data Protection Officer" course; made by EI Pass	The DPO is a high-level professional figure who must be involved in all matters relating to the protection of personal data. He has a high degree of autonomy and is designated on the basis of his professional qualities.	Middle level	The training and certification course consists of the following modules: The DPO: designation, position and tasks New technologies: rights and damages The Digital Administration Code and the latest updates EU Regulation 679/2016 and the new rules on the protection of personal	Feedbacks from revious students

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 PEC, digital signature and archiving of digital documents IT Security	
5) „DPO and privacy officer" course; made by Bologna University	The course offers a training course that aims to: - to train the new professional figure of the "Data Protection Officer" (DPO) or "Data Protection Officer" (DPO), institutionalized by the new EU regulation on the protection of personal data (GDPR, EU Regulation no. 679/2016), as well as other relevant figures (such as: the "Privacy Officer" or employee in charge of privacy functions of companies or public bodies and the Manager of personal data); - offer specific and interdisciplinary training in Data Protection and Privacy to those who already work or intend to work in the fields of privacy, corporate security and IT resource management in companies and public bodies, as an external consultant or as an internal expert.	Graduates currently operating or aspiring to operate as "Data Protection Officers", as "Privacy Officers" (or privacy officers or privacy referents), as Consultants with expertise in the field of personal data protection. Individuals who already operate or intend to operate in the areas of privacy, corporate security and management of IT resources in companies and public bodies, as external consultants or as internal experts.	Right to personal data protection and Data Protection Officer Security measures, data breaches, investigative and web investigations Corporate security, new technologies, impact assessment and application practices Web society, web security, big data and privacy by design	

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.

		Managers or employees of the various company functions (human resources, IT managers, security managers, etc.) who intend to take care of the preparation in terms of personal data protection (privacy), as they are called upon to hold the role of "Managers of the processing of personal data".		
6) „DPO course"; made by Eduforma in Padua	The course will allow you to deepen your knowledge of EU legislation, cyber security and data protection, providing you with the skills you need to embark on the new profession of DPO.	The DPO studies the aspects inherent in the analysis of data and their processing from the computer, legal and organizational point of view. In addition, it analyses communication strategies to involve external and internal clients in data management. It applies problem solving strategies to the solution of managerial problems and,	Module 1 - DATA MANAGEMENT ELEMENTS IN ORGANISATIONAL CONTEXTS (8 hours): Elements of company organization: process analysis and graphic representation Techniques for archiving company data: the document workflow Characteristics of UNI standards	Videos made by teachers and participants

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.

		more generally, to their use as a support to the management of privacy policies. At the end of the course participants will have an adequate knowledge of the rules and practices of personal data management, including in terms of technical and organizational measures or measures to ensure the security of data in the company.	(International standard) Module 2 - NORMATIVE AND LEGISLATIVE ASPECTS ON DATA PROTECTION (48 hours): EU Data Protection Regulation 2016/679 Privacy Policy: Information, Consent and Management of Intellectual Property (IPR) Violation of the rules: Information Offences, Sanctions and Protections The national and international guarantee bodies and supervisory activities of the authorities The role of the DPO in enterprises: supervisory information and audits Risk management strategies and minimum data security measures at national and international level Module 3 - DATA PROTECTION (24 hours):	

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.

			Definition of Information Security: privacy by design and privacy by default Methodologies for the analysis of cyber threats Antivirus systems, Backup and disaster recovery systems Definition of client/server concepts and methodology How Network Protocols interact Online publication of data and information	
7) „Privacy governance: the dpo and other key roles" course; made by LUISS Business School	The new Regulations, in Articles 35, 36 and 37, also define the role of the Data Protection Officer, who must be designated when: the processing is carried out by a public authority or body, with the exception of the courts; the main activities of the Data Controller or Data Processor consist of processing operations which, by	Operators who perform the role of Privacy Manager, Data Protection Officer, IT Manager, Security Manager, Compliance Officer, Privacy Auditor, Privacy Specialist; Freelancers who carry out consultancy activities in the field of data protection;	Several modules that cover all the issues and contents	Feedbacks from revious students

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.

	virtue of their nature, purpose and/or purpose, require regular and systematic monitoring of the persons concerned on a large scale; The main activities of the Data Controller or Data Processor consist in the large-scale processing of special categories of data (sensitive data) and data relating to criminal convictions; where provided for in Union law or in the law of the Member State, a group of undertakings may designate a single DPO provided that it is easily accessible by each establishment. Several public authorities or bodies may designate a single DPO, taking into account their structure and size. In this new scenario, many companies, authorities and public bodies will have to adapt to the new regulations, assigning the function of "data protection officer" within their own structure or to external professionals, who, in addition to a wealth of regulatory knowledge in the sector, will have to ensure advanced knowledge of security and information systems. In addition, the UNI 11697/2017 standard has also	All those who wish to enrich their portfolio of knowledge in the field of Privacy.		

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.

	outlined other profiles relating to the processing and protection of personal data, in order to better manage the governance of data protection. The training course therefore aims to provide the basic knowledge relating also to the figure of the Manager, Auditor and Privacy Specialist.			
8) „Privacy path: obligations, risks and opportunities for companies course"; made by CPV Foundation in Vicenza	The objective of the course is to provide guidelines for the correct application of the new privacy legislation at the company level, both to avoid the new penalties of up to 20 million euros and to reap the benefits in terms of company security, management and monitoring of workers. The course is structured in three courses that can also be purchased individually. Each course specifically analyses different but complementary issues. The course begins with an analysis of the differences and consequences at the company level of the new rules on privacy introduced by EU Regulation 2016/679 applied from 25 May 2018, which has changed the point of view on the protection of personal data, both with regard to the general	The course is aimed at entrepreneurs and managers, privacy and compliance managers, personal, marketing and legal affairs managers, IT and security managers, personal data processors, professionals (lawyers, accountants, employment consultants, business consultants)	Several modules that cover all the issues and contents	No

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.

	principles and the rights of those concerned. A course will follow on a specific part of the new privacy regulations aimed at the protection of personal data. The course concludes with an analysis of the impact of the privacy discipline introduced by European Regulation 2016/679 with effect for workers.			

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

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

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

A close distance from business desires is the Security Analyst (55%), which analyzes potential vulnerabilities of systems, networks and business applications.

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

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

... but SMEs remain vulnerable! In fact, If we analyse the scenario in SMEs, things change radically. While in medium-sized businesses the person in charge of information security is covered by a real IT manager, in small and micro businesses it is the owner himself or the general manager who takes his place.
But what is worrying is the fact that in less than 30% of SMEs there is the figure of a security manager, while in 15% there is no figure to oversee the information security. And it works in particular for ISO and DPO, that are the two main job profiles linked with our project.

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)
1) Head of Cyber Security & Threats Management; for an national insurance company	The Cyber Security & Threats Management has the mandate and the responsibility for managing at global level the IT Security & Cyber Threats activities, implementing solutions and running operations in order to prevent and to manage cyber risks. The manager conceptualizes, organizes, implements the solutions, the procedures and the activities coordinating the units that composed the department. He/ She develops partnership with internal customers across the company. The goal of the activities is to mitigate cyber risks in a proactive way, from prevention and intelligence, to detection and management.	• Solid knowledge and experience with Cyber Threats Management (SIEM / SOC; Threat Intelligence and CERT) • Skills and ability to interact at senior level within Generali management • Degree-level education (Computer Science, Engineering, telecommunication engineering, informatics, mathematics, physics. or equivalent); • Certifications on Information Security (e.g. CISSP, CISM, ISO27001, CISA, ISO22301, GSEC, CEH, CSX etc.) would be a plus; • Experience in technical security domains (network security, application security, data security, cloud security, vulnerability management etc.) would be a plus • Experience on information security governance, IT risk management, regulatory compliance (e.g. Privacy Law) and audit procedures would be a plus • Knowledge of main Information Security standards and framework (ISO27001, ISO22301, ISF, NIST, COBIT etc…) would be a plus <u>Soft Skills</u> • Communication skills and ability to manage a wide array of different stakeholders • Strong operational focus, ability to drive topics and deliver results even under pressure and time constraints • Cross-country team management; ability to work in large international security projects; • Fluent English, another European language is a plus • Integrity • Proactivity, high energy and enthusiasm, with a "hands-on" approach, resilience • Strong interpersonal skills with an ability to effectively influence, persuade across geographies, cultures, markets and levels of seniority • A global mindset Passionate • A "quality-driven" individual • Advanced problem solving, analytical and communication skills; • Strong organizational and project management skills • Demonstrated ability to work effectively as part of a team.
2) Security	The role must guarantee the management	- 2 years of experience in Advisory, Compliance, Governance and Risk management

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.

manager, Junior; for a SME	of Risk Management activities within the Data Protection & Security Management initiatives: the resource will support the Project Managers and DPOs for context analysis, process mapping and the control and management of Data / Security Management activities. The role also includes the drafting of logical, organizational and physical Security Policies and Procedures, as well as the analysis of IT security solutions.	activities, in roles focused on the analysis and definition of information security and data protection solutions. - Master's degree preferably in Law or Management Engineering - Knowledge of English language The key competences of the role are: - knowledge of the GDPR and national regulations in the field of Privacy & Data Protection; - knowledge of methodologies and application of Risk Management and Security Audit; - knowledge of the main standards in the field of Information Security/Data Protection (e.g. ISO/IEC 27000, COBIT, OWASP, NIST etc.); - ICT Security certifications (e.g. CRISC, CISM)
3) IT security specialist; for a trade company	The person will be responsible for maintaining and developing the Information Security framework in order to ensure compliance with all existing IT security policies and procedures and the continuous improvement of IT security standards.	Master's degree in Computer Science or Engineering; Previous experience of at least two years in the field of Information Security; Good knowledge of English, written and spoken; Pleased to have technical certifications on IT Security and knowledge of GDPR and ISO standards related to information security. Preference will be given to having developed expertise in McAfee and Check Point solutions; the profile is completed by determination, precision, and orientation to teamwork and objectives.

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) Chief Information Security Officer; for a Chamber of Commerce	Chief Information Security Officer (CISO) responsible for defining and implementing enterprise-wide information security strategies and programs to protect systems and resources from internal and external threats. CISO will also be entrusted with the responsibility and coordination of the structures in charge of the Governance of Cybersecurity.	Minimum requirements: Degree in Computer Science or similar At least 10 years of experience in IT security, with roles of coordination of activities, projects, work teams, preferably gained within companies or structured companies, in contexts of high organizational complexity. They complete the profile: Certifications in the field of Certified Security Systems Professional (CISSP), Certified Information Security Manager (CISM) or equivalent. Experience in the areas of systems architecture, administration, application development, database administration, network operations and data center operations. Experience with security frameworks such as ISO 27001/27002, CIS Critical Security Controls, NIST Framework. Experience in developing and administering information security policies and procedures in a complex environment. Experience in evaluating controls and systems using a risk-based approach. Experience in forensic investigation methodology for computers and investigative tools for collecting, analysing and storing electronic evidence. Good knowledge of English. Excellent communication skills, leadership and strategic vision, ability to manage negotiation techniques, strong initiative and pro-activity.

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) Junior project manager information security; for a middle size energy company	The resource in particular will be required to: manage and implement relevant projects in the field of Information Security, for the whole life-cycle of the project, from the analysis of requirements to the TAOs up to Go Live; govern the Identity Access management process; have a good knowledge of HR processes in a Group context; have a good knowledge and mastery of GDPR regulatory compliance; contribute to defining and implementing the security policy and standards by aligning them with the ICT strategy; contribute to the development of the cyber security roadmap. The resource will also deal with: define and monitor compliance activities: administering Governance and Identity Access Management tools; manage the developments related to the	You will also need to have a thorough understanding of project management methodologies. Certifications are useful for the purposes of the activities: PMI, ITIL, Agile, ISO27001. Qualification required: Bachelor's degree in computer science, with a preference for computer engineering or computer science. The figure is also required: Strong analytical and problem-solving skills Strong determination Good time and priority management Relationship and integration skills in a dynamic and motivated working group Team-working skills Flexibility and versatility Autonomy and solution and result orientation Good knowledge of English and Office Automation tools required. Request good knowledge of Information Security processes.

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 Privacy activities; analyze and review HR processes; Interfacing with other ICT functions to manage incidents related to identities and access profiles. Check through the tools provided the correct attribution of profiles on corporate file servers.	

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)
1) Junior data protection officer; for a middle size company	Support to the Data Protection Manager in the execution of all the obligations imposed by the European and Italian legislation on Privacy (EU Regulation 2016/679, Legislative Decree 101/2008); Drafting and revision of contracts and privacy policies for the Group's websites; Drafting and revision of appointments as data controller pursuant to art. 28 EU Regulation 2016/679 Analysis of privacy impacts in relation to corporate projects involving personal data relating to users - consumers; Updating of the register of processing operations pursuant to Art. 30 of EU Regulation 2016/679.	Degree in Law or Legal Discipline, preferably not more than 1 year old; Strong interest in privacy and data protection issues; Excellent knowledge of the English language Excellent knowledge of the Office package
2) DPO – GDPR consultant; for a small size	The person will be placed in a working group with specific skills to ensure a real process of accompaniment to GDPR compliance for the hospital	- Knowledge of the new European GDPR legislation - Knowledge of the world of privacy, compliance, data protection and data

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.

consultancy firm	sector.	governance - Previous experience in the health sector - Knowledge of clinical-health analysis processes - Knowledge of the IT world
3) DPO and legal expert; for a consumers national association	Monitor compliance with and compliance with GDPR and data protection/protection legislation; Ensure that the organization's processes regarding personal data and different subjects (employees, customers, suppliers and any other person) comply with applicable data protection rules and internal policies; Be an internal point of reference for all matters relating to the processing of personal data and GDPR; Evaluate the organization with a risk-based approach of the GDPR applications and provide advice where required regarding the Data Protection Impact Assessment (DPIA) and monitor its performance; Act as a point of contact between the organisation and the supervisory authority and communicate and	Professional experience indispensable experience of at least 5 years in particular in the field of privacy, data processing and confidentiality; welcome experience in professional firms specializing in corporate and commercial law. Training Law degree Specialisation or specific training in privacy / data security More than good knowledge of both spoken and written English Skills excellent ability to influence, negotiate and communicate, ensuring the ability to work effectively with people at all levels and externally, with suppliers.

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.

	cooperate with the latter.	
4) DPO expert/senior; for a world wide insurance compaby	The Data Protection Officer ("DPO") for the EMEA (Europe, Middle East and Africa) region must have expert knowledge of global data protection laws and practices and individual data subject rights, in addition to technical and organizational measures and procedures. The DPO must possess a mastery of technical requirements for privacy by design, by default and data and information security. The DPO must be able to balance the role of a trusted advisor to the company as well as be able to interact with executive level leaders of the firm, and data protection regulatory authorities from time-to-time.	• Bachelor's or Professional Degree . • Financial services experience. • Significant (5-10 years) experience in • EU and global information security and data protection laws, including drafting of data protection policies, technology provisions and outsourcing agreements. • Change Management • IT Operations and Programming, including attainment of information security standards certifications and data protection seals/marks. (e.g. CISSP, CISA, etc.) • Information systems auditing, attestation audits and the assessment and mitigation of risk. • Must have experience acting in an independent manner; prior experience in professional services with client relationship and audit background to handle the delicate task of discovering gaps, encouraging gap mitigation, and ensuring compliance without taking an adversarial position. • Will possess leadership and project management experience, to be able to request, marshal and lead the resources needed to carry out their roles. • Should have broad business experience to know the reinsurance and insurance industries and the roles of the data controller and processor well enough to understand how data protection should be implemented to integrate with the way each company designs and markets its products and services and earns its revenues. • Demonstrated leadership skills achieving stated objectives involving a diverse set of stakeholders and managing varied projects. • DPA Negotiation skills and the ability to speak with a wide-ranging audience, from the board of directors to data subjects, from managers to IT staff and lawyers. • Demonstrated record of engaging with emerging laws and technologies.

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.

		• Experience in legal and technical training and in raising awareness. • Client relationship skills and the ability to continuously coordinate with controllers and processors while maintaining independence. • EU residency and must be independent of real and perceived conflicts.
5) Data protection consultant; for a IT and consultanty firm	legal to be included in the Audit & Control area to support the team that provides the service of "Data Proection Officer as a service" in the activities of specialist legal advice and execution of audits to verify compliance with regulations on the protection of personal data.	3/4 years of experience specifically on issues of personal data protection, and in the planning and execution of internal controls of regulatory compliance Interested in gaining experience in the DPO function in medium and large companies Good knowledge of English language Excellent knowledge of Office package Availability for travel It is a preferential requirement to have attended postgraduate training courses in the areas of internal auditing and data protection.

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

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

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

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

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

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

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

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

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

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

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

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

5) Microsoft MCSE: Cloud Platform and Infrastructure;

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

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

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

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

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

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

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 UNI 11697:2017 standard defines four professional profiles relating to the processing and protection of personal data:

1) Personal data protection officer (DPO): a figure governed by art. 39 of EU Regulation 2016/679 which supports the Data Controller or Data Processor in the application of the regulation and ensures its observance.
2) Privacy Manager: figure who coordinates across the subjects involved in the processing of personal data, in order to ensure compliance with applicable laws and the achievement and maintenance of the appropriate level of protection based on the specific processing of personal data carried out.
3) Privacy Assessor: an independent figure with knowledge and skills in the IT/technology sector and of a legal/organisational nature who conducts audits on the compliance of personal data processing using, if necessary, specialists in both areas.
4) Privacy Specialist: "operational" figure who supports the DPO and/or the Privacy Manager in developing appropriate technical and organizational measures for the purposes of processing personal data and ensures the proper implementation of the processing of personal data.

The certification scheme for privacy profiles has been set up in accordance with the UNI 11697:2017 standard and developed on the basis of the UNI CEI EN ISO/IEC 17024:2012 accreditation standard.
The certification process for candidates is divided into the following steps:

- submission of the application, using the "certification request" form and all the required documents;
- verification of possession of the requirements of education and professional experience required;
- carrying out of a certification examination, consisting of written tests and an individual interview on professional subjects;
- issue of the certification by the deliberation committee.

The certification for each privacy profile is valid for 4 years with tacit renewal.
The validity of the certification is subject to compliance with the conditions required by the scheme for its maintenance.

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.

Other important issues regarding the topic of the report

We should consider that, in Italy, around 98% of the whole companies are small or micro businesses. So, even if the National or European laws and regulations are quite strict and well defined, in the "real" world we should take in consideration that:

- private and public bodies, quite often, offer training courses that are planned for big size companies or public administrations;

- above all for micro businesses, there is a key role of trade associations that are offering short term (and quite cheap) courses for entrepreneurs and professionals;

- in the same time, there are thousands of free lancers (IT experts, consultants, trainers and ex managers) with a wide experience in the project field, that are offering not only theoretical contents but also a sort of „facilitating service";

- this kind of approach is connected with i.e.: how to „translate" (from the laws/regulations into the business language) the key elements in practice; how to motivate all the company team (and not only the owner/manager) on the information security and data protection contents; how to find public funds (i.e. from ESF - European Social Fund) for supporting the training costs, etc.

We should also take in cosideration that, basically, project is focused on non-formally and informally learning. So, all the report paragraphs content possible ISO and DPO profiles, that market requestes at the moment.

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.

Executive Summary and Resume

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

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

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

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

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

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

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

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.