Funded by the
Erasmus+ Programme
of the European Union

TeBeISi

IO 1

Annex 1 - Cases collected from field research

Report on Identification of Competence Profiles

Funded by the
Erasmus+ Programme
of the European Union

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

.

Funded by the
Erasmus+ Programme
of the European Union

Cases collected from expert interviews

In August and September 2019, the partnership interviewed more than 60 experts in the fields of Data protection and Data security, Information security and IT security in small and medium-sized enterprises (SMEs). It was important to us to gather personal opinions and experiences on these topics (either individually or in focus groups).

The aim of our interviews was to gain a deeper insight into the need for SMEs to employ personnel in the field of information security. We have taken a lot of time for the surveys in order to gather as much information as possible - including informal information. This should enable us to find the most comprehensive picture possible of information and data security in everyday professional life.

Some examples of questions are:

- What causes an acute need?
- How acute (in terms of time) is it?
- Which areas and processes are affected by this need?
- Which competences are relevant for the occupational field?
- What strengths and weaknesses do you see in yourself and your employees?
- What problems do you encounter in your daily work environment?
- What tips can you give us for our project?

As was already the case for desk research, national reports were written for field research, which illustrate the country-specific results in detail. An important result of the field research is that at least 10 concrete case studies from practice were documented per country. These cases then formed the basis for the collection of required / desired competences in both fields, Information Security and Data Protection.

We present the single cases of each participating country on the next pages:

Tasks	Planning Activity	Running Activity	Manage Activity	Skills / knowledge / competencies required
Candidate_01_DE: **Implementation of a new structures in the firm**	Planning security and protection involves a high level of abstraction, especially when it comes to requirements. What is the input and output available? How large is the availability of resources? Planning these things represents the foundation for later actions. A measure to raise security is also about identifying critical processes and "hiding" them among other routine tasks in the firm.	Tasks are mostly routine, like Patch- and Update Management.	Crucially, having systems in place to ensure that inly the right people have access to certain information or processes, i.e. identity and access management. This involves review and paying attention to personnel security. Of course, this task is dependent on other variables: HR, leadership of the firm and the Budget.	See table of contents ISO 27001: -Leadership -budget procurement -communication skills -Planning -operation: ITIL -process knowledge & modelling -management skills -Personnel security -Responsibility for values (Determination of protection requirements) BSI: IT basic protection ➔ write guidelines Describe training
Candidate_02_DE: **ISO: Establishment of an ISMS:** **4 steps: 1) As-is analysis: documentation of all providers, processes, contracts etc.** **2) Protection requirement analysis:**		You need to be able to trigger new processes which involve activities tangent to your	Most importantly, an ISO needs to write and implement regulations, measures and	Must haves: - IT-Know How - Project Management (Reporting, implementing measures etc.)

Grouping of As-Is analysis into processes. Identification of most important processes. 3) Risk analysis: What needs to be done to ensure the protection of these processes? 4) Measure implementation: decision about which measures are to be implemented by the IT department and which will be assigned to external experts.		employees workflow, i.e. change management. Then you need to be constantly aware of thread potentials and know possible impacts on the firm and how to prevent them (risk management)	guidelines in order to substantiate his position if a breach occurs.	Nice to have: - Legal knowledge (GDPR) - Certification ISO 27000 - Soft Skills (mediation, "selling", sensitivity) Further: - self-motivation - communication skills - Service-mentality
Candidate_03_DE: **Consulting firms in questions of information security**	Dependent on the size of the firm. In a small company, people tend to have a 360 degree perspective, and dispose of more basic technology. In a larger company, the systems are more complex and employees only need to think from A to B.	We have two kind people: the one hand there is the "teckie", who disposes of very profound technical knowledge and who really likes to go into detail and to develop existing topics. Then there are the rather business oriented people, who like information systems and looks at problems from a more universal perspective. Tasks involve formation, implementation of ISMS and consulting.	People need to communicate effectively with clients.	We have must-have criteria. Aspects which we don't consider mandatory are not even included in our job ads. Generally, applicants dispose of a university degree, but we made equally good experiences with people who come from a more "technical background", and who gained knowledge through working experience. Primarily, the applicant needs to have any sort of education. Then we check if he or she has certificates, which one and when they were granted. Finally, we look for working experience. If people don't have any working experience at all, we categorically reject their

				application. In a personal call I then check for personal, methodological and social treats which are necessary for an advisor.
Candidate_04_DE: **Implementing IT security based on ISIS 12**		We conduct awareness campaigns and help to implement ISIS12, explain the necessary steps and why they are necessary and what the expectation of the management is.		Willingness to learn new methods, be able to build a connection with people and to be capable to establish your opinion. The latter might even be the most important one. It is quite easy to teach technical aspects of the job, but much more difficult to change the personality of someone.
Candidate_05_DE: **Increase the level of information security in the firm**	Develop a play of what needs to be secured, how to do it and which actors are involves.	Sell ideas to the head of the firm and be aware of the extra work which is entailed for the IT department.	The most important process Is risk management.	For us, the most important aspect, despite social competences, is that the person shows the willingness to learn, to travel and to have a customer oriented mindset.
Candidate_06_DE: **Respond to new challenges due to**	As a specialist department, you	Implement clear rules for the	We try to limit the usage of	The person needs to think

technological changes: employees who are used to applications from private use need to have practical alternatives for their work, which ensure information security and data protection, like private clouds or internal chat applications.	need to develop a strategy of how you aim to achieve the security of the firm, and to sell this strategy to the company lead. You need to think about certain scenarios and how you want to react to them. You need to be able to avoid situations, in which a threat materializes and your department gets involved if it is already too late.	usage of business and private communisations. I would lie if I told I would make attempts to convince our employees. We simply lay out the rules: the same way, that nobody brings his or her playstation,	applications like WhatsApp or Cloud Storage by providing own alternatives.	analytically. The person needs to be ready to continuously develop, especially in terms of knowledge about threads. The person needs to maintain a high routine in her workflow.
Candidate_07_DE: **Ensuring Information Security:**	Analysing possible scenarios: It is a crucial point to think about incidents which can occur and to reason “How can I protect myself? Are there scenarios which I can prevent before they occur? What do I have to do after they occurred?”. Thinking about what can happen and what needs to be done, and to establish processes to be able to react if they occur.	Daily critical analysis: “Asking yourself: “What can I improve?” Possible solutions have to be documented.	Risk management: “Not only pecuniary aspects play a role, but also the likeliness of an incident to occur. At a certain point, there is nothing you can do to prevent an incident from happening. I can’t protect myself from someone to sit in front of a PC who remembers three dates, walks out and writes them down. So you need to assess: “What happens, if such a breach occurs? How large would be	University degree and Legal understanding “Maybe a legal education in combination with IT”.

			the inflicted damage?" You need to see whether criminal energy is in play and if damage occurs only in isolated cases. Another thing would be if someone would steal costumer data with a USB stick. The damage would be large because many clients would be involved.	
Candidadate_08_De: **Take care of black sheep within the company and provide help if people are not sure how to carry out their task appropriately.**		Ensure that employees keep following the established processes: Conduct internal employee trainings and keep people aware of the importance of information security. People are convenient and if you charge them with additional tasks, they stop doing them at some point.	Communicate with corporate management: We don't need to conduct cost-benefit calculation, because we simply need security technology and a functioning EDP, so there is no need for any discussion. Categorically, technology comes first and the costs are being accepted, even if it is costly.	Formation and education are important, but not on top of the list. I would say experience! You need to be able to estimate risks, and that means you need to know the users. You need to know where needs are, where further education is needed and where to trigger processes. Experience with methods and as well as with colleagues to me is most important.

Candidate_9_DE: **Implementation of an ISMS as well as ongoing control, updating and improving of existing processes.**	Foresee contingencies and write a guideline of what needs to be done and who is in charge.	Implement an Information Security Management System. It is important to dedicate time to keep it running, update and implement new processes if necessary, control if all employees are aware of guidelines and whether the processes are adequate to meet new challenges.	Maintain a good relationship to all employees end ensure their awareness for potential risks. Every employee should know, what he or she can do to contribute to the security of the firm.	Most importantly: IT Know-How. But also knowledge of project management, i.e. how to implement measures and reporting. For us, it is nice if people bring legal knowledge to the table, like the GRDP or knowledge about ISO 27000.
FG_01_DE: **The more specific a task, the more likely it is to be purchased from external providers.** **The most relevant aspects were Password Management and Customer Communication.**		Customer Profiles, Account Data, Telephone/Fax/ Mailing lists, Recruiting, advertise campaign, database, Maintenance, Customer Service, R&D, Sells, Payroll Accounting, Patents and Trademark	Password Management	Qualifications (white): University Degree; Degree or Certification of: Information Technology (IT) / Programming / IT Security / Computer Science / IT Administration / Data Security / ITIL Experiences (Orange): Programming; Practical Experience with Security Vulnerabilities; System Rollout and Implementation;

				Documentation; Consulting; Accounting; Employee Briefing; Server Administration; System Recovery Knowledge (Green): Change Management; Legal Background; Java; IT Security; IT Solutions; Security Vulnerabilities; Server Architecture; IT Grundschutz (Germany); Linux Skills and Competences (Pink): Fast Familiarisation with new Topics; Risk Assessment; Firewall Implementation; Experience with Exchange Server; Self- Motivation; Virtualisation; Statistics and Analysis; Awareness of new Topics; Ability to Cope with Pressure (Toughness); Resilience; Server Implementation; Personal attributes

FG_02_DE **Business Continuity Management and Password Management represent the most important aspects of an ISO.**		Procurement (Development Operations), Influencing, Data retention and processing, encoding, Role Based Access Control (RBAC), Software and project leadership (defend extra costs for new software to meet stricter requirements)	Business Continuity Management, Password Management, Behavioural Management, Process Management	Skills: Assertiveness, App-Development, Analytical thinking and structured workflow, Knowledge of human nature, persuasiveness, Risk assessment, readiness to travel, working independently Knowledge: Network technology, IT-knowledge, understanding of the product/production, legal aspects, IT Basic Protection, Communication and Moderation Qualifications: Information Systems (Application), IT-Administration; Computer Science, University Degree (Business Administration, Computer Science, Information Systems), legal training with information Systems, Project Management,

				ISO 27001 (Foundation, Auditor), Certificates Experience: Encoding and system support (general IT support), 3 years of working in IT and Process Management, Process Thinking, ISMS Projects, practical experience with security breaches, 5 years of general working experience, Processing external sensitive data, systematic thinking

Tasks	Planning Activity	Running Activity	Manage Activity	Skills / knowledge / competencies required
Candidate_01_IT: **First assessment phase: how to improve the level of awareness, about IT security and data protection in the micro and SMEs**	- first meeting - interview through a detailed questionnaire - first feedback report	- constant dialogue with the client - reply to specific legislation (i.e. GDPR) questions, etc - first assessment report and knowledge gap	- exchange with the owner / director - definition of the main strategy	- All employees are trained in the basic knowledge of GDPR. - HR and soft skills - Managers standing behind the idea - Employees awareness - Data security awareness (all)
Candidate_02_IT: **Assessment phase and intervention: how to improve the level of awareness, about IT security and data protection in the micro and SMEs, how to measure the gaps (in term of knowledge and procedures); how to implement the actions**	- first meeting - interview through a detailed questionnaire - first feedback report - definition of an implementation plan - follow up and check	- constant dialogue with the client - reply to specific legislation (i.e. GDPR) questions, etc - assessment report and knowledge gap - weekly meetings for the assistance - follow up	- exchange with the owner / director - definition of the main strategy - middle term plan	Operational security - HR and soft skills - Managers - software development team - solution architects - IT developers who understand the needs of employees - IT security and data manager processes All employees are trained in the basic knowledge of GDPR.

Candidate_03_IT: **The certification of knowledge and skills in the areas of information security and data protection is carried out by a large number of providers, but the content of the learning and the examination certificate are not standardised or accessible to all**	- first meeting - interview through a detailed questionnaire - first feedback report	- 24 hours course	- definition of implementation plan	- HR - software development team - solution architects - IT developers who understand the needs of employees - IT security and data manager processes - All employees are trained in the basic knowledge of GDPR.
Candidate_04_IT: **External cyber attacks - employee captures or erases data for revenge**	- risk analysis - meetings - implementation of safety contents	- constant dialogue with the client - reply to specific legislation (i.e. GDPR) questions, etc - assessment report and knowledge gap	- definition of the main strategy - middle term plan	- HR - software development team - solution architects - IT developers who understand the needs of employees - IT security and data manager processes - All employees are trained in the basic knowledge of GDPR
Candidate_05_IT: **APP construction in the field of sustainable mobility**	- meetings with providers - world wide legislation (not only GDPR) analysis	- set of options - costs / benefits analysis - operations planning	- middle term sustainability	- Understanding the GDPR (probably with the help of experts in this field)

				- Programmer - Privacy expert from a client - Awareness rising within my network
Candidate_06_IT: **Information security (medical records)**	- meetings with providers - legislation (GDPR) analysis	- verification of the proper functioning of equipment, software and processes. - Updating security standards in existing programs	- carefully identification of company needs, planning change in relation to needs, informing users at various levels	- HR - software development team - solution architects - IT developers who understand the needs of employees - IT security and data manager processes
Candidate_07_IT: **Set up of a security plan in a client (SME)**	- first meeting - interview through a detailed questionnaire - first feedback report - definition of an implementation plan - follow up and check	- constant dialogue with the client - reply to specific legislation (i.e. GDPR) questions, etc - assessment report and knowledge gap - weekly meetings for the assistance - follow up	- exchange with the owner / director - definition of the main strategy - middle term plan	- HR - software development team - solution architects - IT developers who understand the needs of employees - IT security and data manager processes - Programmer - Privacy expert from a client

Candidate_08_IT: **- Security Policy Document (if any) or documentation equivalent (Privacy Organigram, Treatment Register, etc.)** **- Policy on the use of company tools for data processing**	- first meeting - interview through a detailed questionnaire - first feedback report - definition of an implementation plan	- constant dialogue with the client - reply to specific legislation (i.e. GDPR) questions, etc - assessment report and knowledge gap	- exchange with the owner / director - definition of the main strategy - middle term plan	- All employees are trained in the basic knowledge of GDPR. - HR and soft skills - Managers standing behind the idea - Employees aware of the importance - Data security awareness (all people involved)
Candidate_09_IT: **Data Protection Assessment of ICT resources (Gap Analysis).**	- first meeting - interview through a detailed questionnaire - first feedback report - definition of an implementation plan	- constant dialogue with the client - reply to specific legislation (i.e. GDPR) questions, etc - assessment report and knowledge gap	- exchange with the owner / director - definition of the main strategy - middle term plan	- All employees are trained in the basic knowledge of GDPR. - HR and soft skills - Managers standing behind the idea - Employees aware of the importance - Data security awareness (all people involved)
Candidate_10_IT: **First data protection assessment, in a legal office**	- first meeting - interview through a detailed questionnaire	- constant dialogue with the client - reply to specific legislation	- exchange with the owner / director - definition of the main	- HR - software development team - solution architects

	- first feedback report - definition of an implementation plan - follow up and check	(i.e. GDPR) questions, etc - assessment report and knowledge gap - weekly meetings for the assistance - follow up	strategy - middle term plan	- IT developers who understand the needs of employees - IT security and data manager processes - All employees are trained in the basic knowledge of GDPR.
Candidate_11_IT: **Drawing up of the treatment areas allowed to authorized employees and collaborators** **(e.g., authorisation for access to information technology resources and paper documents);**	- first meeting - interview through a detailed questionnaire - first feedback report - definition of an implementation plan - follow up and check	- constant dialogue with the client - reply to specific legislation (i.e. GDPR) questions, etc - assessment report and knowledge gap - weekly meetings for the assistance - follow up	- exchange with the owner / director - definition of the main strategy - middle term plan	- HR - software development team - solution architects - IT developers who understand the needs of employees - IT security and data manager processes - All employees are trained in the basic knowledge of GDPR.
Candidate_12_IT: **Drafting or updating of letters of appointment of internal processors**	- first meeting - interview through a detailed questionnaire - first feedback report - definition of an implementation plan	- constant dialogue with the client - reply to specific legislation (i.e. GDPR) questions, etc - assessment report and knowledge gap	- exchange with the owner / director - definition of the main strategy - middle term plan	- Operational security - HR and soft skills - Managers -software development team - solution architects - IT developers who understand the needs of employees - IT security and data manager processes

				All employees are trained in the basic knowledge of GDPR.
Candidate_13_IT: **Drafting of appointment/contract letters for external data processors (such as provided for by the European Regulation)**	- first meeting - interview through a detailed questionnaire - first feedback report - definition of an implementation plan	- constant dialogue with the client - reply to specific legislation (i.e. GDPR) questions, etc - assessment report and knowledge gap	- exchange with the owner / director - definition of the main strategy - middle term plan	- solution architects - IT developers who understand the needs of employees - IT security and data manager processes - knowledge of GDPR. - HR and soft skills - Managers standing behind the idea - Employees aware of the importance - Data security awareness (all people involved)
Candidate_14_IT: **Compliance with the Website (drafting / updating of the Privacy Policy and Cookies** **Policy, ad hoc information for contact request).**	- first meeting - interview through a detailed questionnaire - first feedback report - definition of an implementation plan	- constant dialogue with the client - reply to specific legislation (i.e. GDPR) questions, etc - assessment report and knowledge gap	- exchange with the owner / director - definition of the main strategy - Middle term plan	- solution architects - IT developers who understand the needs of employees - IT security and data manager processes - knowledge of GDPR - HR and soft skills - Managers standing behind the idea

				- Employees aware of the importance - Data security awareness (all people involved)
Candidate_15_IT: **Data Protection Impact Assessment (DPIA) on new treatments**	- first meeting - interview through a detailed questionnaire - first feedback report - definition of an implementation plan	- constant dialogue with the client - reply to specific legislation (i.e. GDPR) questions, etc - assessment report and knowledge gap	- exchange with the owner / director - definition of the main strategy - Middle term plan	- HR - software development team - solution architects - IT developers who understand the needs of employees - IT security and data manager processes - All employees are trained in the basic knowledge of GDPR - Managers standing behind the idea - Employees aware of the importance - Data security awareness (all people involved)
Candidate_16_IT: **Verification of the requirements of Privacy by Design and Privacy by Default on the new tools and processes for the processing of personal data**	- first meeting - interview through a detailed questionnaire - first feedback report - definition of an implementation plan	- constant dialogue with the client - reply to specific legislation (i.e. GDPR) questions, etc - assessment report and knowledge gap	- exchange with the owner / director - definition of the main strategy - middle term plan	- Operational security - HR and soft skills - Managers -software development team - solution architects - IT developers who understand the needs of employees

				- IT security and data manager processes All employees are trained in the basic knowledge of GDPR.
Candidate_17_IT: **Periodic risk analysis and verification of security measures (in a small business Association)**	- first meeting - interview through a detailed questionnaire - first feedback report - definition of an implementation plan	- constant dialogue with the client - reply to specific legislation (i.e. GDPR) questions, etc - assessment report and knowledge gap	- exchange with the owner / director - definition of the main strategy - middle term plan	- All employees are trained in the basic knowledge of GDPR. - HR and soft skills - Managers standing behind the idea - Employees aware of the importance - Data security awareness (all people involved)
Candidate_18_IT: **Internal Audit following the ISO 19011 guide lines (in a small business)**	- first meeting - interview through a detailed questionnaire - first feedback report - definition of an implementation plan	- constant dialogue with the client - reply to specific legislation (i.e. GDPR) questions, etc. - assessment report and knowledge gap	- exchange with the owner / director - definition of the main strategy - middle term plan	- Operational security - HR and soft skills - Managers - software development team - solution architects - IT developers who understand the needs of employees - IT security and data manager processes All employees are trained in the basic knowledge of GDPR.

Candidate_19_IT: **Appointment to Privacy Manager with constant support in the company for defined periods (in a local business center)**	- first meeting - interview through a detailed questionnaire - first feedback report - definition of an implementation plan	- constant dialogue with the client - reply to specific legislation (i.e. GDPR) questions, etc. - assessment report and knowledge gap	- exchange with the owner / director - definition of the main strategy - middle term plan	- solution architects - IT developers who understand the needs of employees - IT security and data manager processes - knowledge of GDPR. - Managers standing behind the idea - Data security awareness (all people involved)

Tasks	Planning Activity	Running Activity	Manage Activity	Skills / knowledge / competencies required
Focus group_01_LT: **Candidate_01_LT:** **Candidate_02_LT:** **Candidate_03_LT:** **Candidate_04_LT:** **Candidate_05_LT:** **Most relevant problems are: protection of clients' personal data; protection of employees' personal data** Subjects thought that their companies are not really good prepared in administration of the provision of social services; Use of ICT in accordance with data protection law; protection of clients' personal data; protection of employees' personal data As we work with a sensitive group, a major problem arises in sharing information within the institution with other staff and providing information to the families /	Prepare memos, what information, to which authorities we can provide. Hire an institution to prepare data and information security documents. In-service training on data protection for all employees Develop a client image disclosure policy to publicize the company: when to take photos, when and where to share photos.	Signed contracts with employees for information security. Adaptation employees' workstations to protect documents (safes; lockable room doors, etc.); Introduce each employee to the company's internal data protection policies, such as door locking, document retention, confidentiality and customer disclosure. Inform each employee of: what data to store; where violations are, and provide protection. Confidentiality and industrial relations and after work. Prepare central databases of	Raising awareness among staff and other institutions The personal data protection information is published in a separate section on the institution's website, which provides information on the personal data protection officers and procedures in place.	Legal knowledge; knowledge of the application of data protection law; knowledge in the field of personal data protection; knowledge of the Regulation and other data protection instruments; knowledge of documentation (archiving); clerical (computer) knowledge. Skills and Competences: Document analysis; collect and process personal data; analytical thinking; communicability; ability to apply legislation; ability to manage information systems; ability to collect data; ability to ensure confidentiality; responsibility.

relatives of the residents for their involvement. Problems arise when working with other institutions: how much information we can provide about our residents. All information on residents' files should be kept confidential. Employees leave residents' papers on their desk.		information. Implementing more training for employees		
Focus group_02_LT: **Candidate_01_LT:** **Candidate_02_LT:** **Candidate_03_LT:** **Candidate_04_LT:** **Candidate_05_LT:** **Candidate_06_LT:** **Candidate_07_LT:** **Candidate_08_LT:** **Subjects thought that their companies are not really good prepared in new customers search; electronic information dissemination; legal and natural persons data protection features.** The most pressing problems are: how to	Agree with each other what information can be disseminated, to whom and from what sources; Improve the qualifications of employees on the GDPR Regulation	General information on information and data protection is provided on the Company's "Customer Information" section; Data security information is provided when sending e-mails; The website provides this information.	Sign confidentiality agreements with employees and clients Familiarize employees with the company's internal information and data protection procedures	Knowledge: Public Relations; basics of law, legal knowledge; knowledge of the curated field; high moral standards. Skills and Competences: Communicative (communication with the customer, customer service); application of legal knowledge in practice; ability to create and use social networks; clerical knowledge; responsibility; problem perception; ability to adapt information to company needs;

search for new customers when all customer data is stored; What information can be disseminated electronically. Dissemination of electronic information; compilation of data; data protection features of legal and natural persons; hide personal information to avoid paying for services. The subjects felt that their companies were not well prepared for finding new customers; dissemination of electronic information; data protection features of legal and natural persons.				ability to work in a team; ability to think critically.
Interview Candidate_01_LT **Information security in institutions, irrespective of their size, is of immense importance as they handle human data.** Small organizations work with sensitive data. Legal regulations and realities encourage certain organizations to be more compact, which allows them to specialize in certain areas.	The organization understands internally the need to save and work with information in an orderly manner, that is to say from the collection, use and storage of information to third parties.	It all depends on the information available. The titles (management, administrator) do not mean much, competencies are very important. So whether to be named administrator or manager at any level there should be people who really understand what they are	Biggest organizations have data protection officers. Their role is often intermediate between the manager and the administrator. They often act as mediators between the outside and the internal, and at the same time, within the institution, oversee the processes of information	Legal knowledge is very important. Knowledge and skills in information technology are also important.

		doing, understand what material they are working on, where that material is, that data is being used.	protection and personal data protection.	
Interview Candidate_02_LT **Keeping employees informed is crucial, as most employees in the organization have only heard about personal data protection, but not exactly know what and why.**	One of the most important activities in the process planning is clear plan formation and clear information and training of employees.	The most important thing is the proper processes, their simplicity and clarity	Control optimization, monitoring and business process monitoring / testing, evaluation, adaptation, application optimization, contingency planning (fees, evaluation). Control optimization, clarity in monitoring and monitoring of business processes are important.	Legal education, strategic and managerial thinking, good communication skills, ability to communicate complex information in clear, understandable language to employees of all competencies are advisable.
Interview Candidate_03_LT **Recruitment; disclosure of data to third parties; contracting ...**	Know how to apply, plan, if i don't know, where to find or at least consult and get the relevant help.	The same as planning, relationship and communication with the team	Organizing work rightly, organizing functions, managing crisis situations, "do not interrupt" others, especially with excessive control	Has a lot of ...as the BDAR law was introduced, people should take a lot of time to improve the knowledge, most of the personal time, not being delegated to courses or training. The thing is a wish: responsible, receiving manager support and permitting training ...knowledge

				of legislation, decisions, decisions, documents, it literacy ....
Interview Candidate_04_LT: **Information management requires technical, administrative, and legal measures to keep organizations operational. Information is the most valuable object in the service sector. It is the key for a successful service provision.** The areas were processes cannot be controlled in physical space (healthcare data, digital financing) will be most fragile since sensitive data management will be more resource demanding.	All, all the procedures, competencies and responsibilities, related with information security, need to be documented within the organization. In planning, incident control or possible outcomes management scenarios need to be confirmed at the basic level of information security regulation (what can be done, what cannot be done, and what is crucial to be done).	Instead of coping with increasing amount of data, organizations should focus on reduction of informational records stored. This only could be achieved through practice by tracking the processes within the organization and trying to optimize them.	Change management need to fall under responsibilities of management level operatives. It means that all legislative and policy changes needs to be integrated within the organizational fabric to keep processes smooth and personnel ready for any requirement that occurs from the outside of organization. Agreements with third party service providers should be maintained since they serve as party of information exchange.	The company gets to hire a lawyer or a technician (ICT specialist) to work as information security officer. Technicians should be educated on legal knowledge, lawyers – to have their IT skills developed to balance the need for information security. It's an interdisciplinary position between law and ICT. Practical experience is a priority. Formal education – second most important factor. Certification is necessary in order to prove basic knowledge in the field. Certificates should be mandatory for managerial positions. - Empathy and ability work in teams were specified as most important social skills.

Tasks	Planning Activity	Running Activity	Manage Activity	Skills / knowledge / competencies required
Candidate_01_AT: **Penetration Testing** – This is done by professional hackers who are responsible for testing the security of companies' IT systems. These tests are performed to detect vulnerabilities and system weak points so that they can be remedied before any actual hackers attack a system and steal sensitive records. By our last penetration tests, it was determined that employees were leaving insecure ports open to instances of our cloud platform. If a hacker had found these, our entire cloud platform could have been compromised.	Managers will determine whether or not this testing is necessary and will plan this with either internal IT security team or an external firm which specializes in IT security. Determine which systems should be tested as determined after discussions with both our dev/ops team and solution architects because they understand the systems best. We must also determine who is responsible for fixing the flaws once they are found.	Carrying out the penetration tests. Making change requests and submitting tickets to the appropriate people or organizations if flaws are found. Implementing more training for employees in case of systematic flaws, such as seen with the insecure ports.	Regular penetration testing to ensure there are no more security flaws to be found. Process in place to quickly correct the flaws.	- Operational security - professional hackers - Managers -software development team - solution architects -dev/ops
Candidate_02_AT: **Password Management has to be improved** Password management is still a key issue when it comes to data and system security. Although we do not have post-it	We plan this activity together with our IT Administration as well as the HR Department. Awareness rising among employees is very important; otherwise the best system will fail.	System administrators will implement a pilot version and Key users (people with advanced knowledge of company processes) will	When we implement the new system we need to involve all managers. They are responsible in their respective areas of User awareness and	- Software requirement - Operational security - Managers standing behind the idea - Employees aware of the

with passwords on the computers anymore, employees (even managers) often take down passwords. This represents one of the highest risks.	It sounds hard to say that, but the biggest threat is usually the person in front of the computer.	advise them and will test the new Password Management System.	further training of their Employees (together with HR), the System administrators and the IT Support Team.	importance - IT developers who understand the needs of employees - Data security awareness (all people involved)
Candidate_03_AT **Unsafe sharing of sensitive/valuable information with 3rd parties in the development process.** In our company we follow very strict guidelines and our employees are regularly trained. One problem we are currently working on concerns the exchange of sensitive technical product development data with 3rd parties. Specifically, it is about familiarizing these external companies with our standards and securing our systems even better.	ANALYSIS: How does the 3rd party receive and store information. We plan to set up secure data-transfer protocols. How aware are employees of this 3rd party? We think of offering short training on Data Security before we share our data. (AWARENESS RISING) IT-Security: We plan to keep as much data as possible in our systems and will expand the accesses of external and make them more secure. All this without affecting the cooperation. This is a challenging task that will accompany us for the next more years.	Work within a walled garden of software and employees. Keep control of spread of information. Block and deter use of unsafe sharing practices. Safe sharing practices, secure data transfer protocols, data security management, central databases and much more.	All of our employees, contingent workers, and subsidiaries are required to abide by our Privacy Statement and to adhere to internal policies, standards, and guidelines regarding our overall data protection requirements and Privacy Principles: • Be transparent about our actions and intent • Present individuals with clear and actionable choices • Practice purposeful collection, use, and retention of data	Teams from these departments: • Product Development • IT-Security • Data-Security • Product Managers • HR

			• Use data for the purposes for which it was collected • Only share data with third parties in limited and approved ways • Be accountable for enforcement of these Privacy Principles	
Candidate_04_AT: **Organisation of afternoon care in schools:** As I have already described above, through the GDPR, we had to prohibit our employees from using WhatsApp to communicate with parents. This caused a lot of excitement on all sides.	We are currently looking for a communication solution that meets the current requirements of the valid guidelines. Several tools are under discussion, but are still under review. If these do not meet the requirements, we are thinking about having a comprehensive app programmed.	As soon as we have found or developed the appropriate tool, we will offer training and inform all employees accordingly. In addition, the parents are informed about the innovations through the schools.	The most important thing is that the management stands behind the new tool and it is constantly being further developed. In order to check the success or analyse the difficulties, experts must be appointed who can take over this task.	In our institution we need the support from the following departments: * HR * IT * Managing Director * External help for App programming if needed
Candidate_05_AT: **The open entrance doors** It may sound ridiculous, but one of our main problems at the moment is to draw employees' attention to their misconduct	We have clear policies, standards and training. However, many employees find compliance too cumbersome. After the moth "Nothing will	* We will intensify training on both data protection and information security. * We will also use "minor penalties" to draw employees'	Our management team must lead by example and take the issue seriously. We will have to keep checking	In our institution we need the support from the following departments: * HR / PD * IT

regarding “open doors”.	happen", even in departments that process highly sensitive data, all doors are regularly left open. Of course, it is convenient not to have to lock and unlock all the time. But we can no longer accept this real security gap and will intensify training on both data protection and information security.	attention to misconduct. For example, not locking the door means donating one euro to the fruit basket. * Working group that draws attention to common misconduct in a humorous way, e.g. small comics.	until all employees have got used to the barrier. We still have “real” keys in some areas. It would be worth considering modernizing these rooms with the card system.	* QM
Candidate_06_AT: **Current problem: Open ports** An open port is an attack surface. The daemon that is listing on a port, could be vulnerable to a buffer overflow, or another remotely exploitable vulnerability. Important principle in security is reducing your attack surface and ensuring that servers have the minimum number of exposed services.	Some thoughts in **C,I,A:** **Confidentiality:** Open ports (actually the programs listening and responding at them) may reveal information about the system or network architecture. **Integrity:** Without open port controls, software can open any candidate port and immediately communicate unhindered. **Availability:** The network stack and the programs at open ports, even if the requests are invalid, still process incoming traffic.	Closing unused ports is like shutting the door on cyber criminals. That’s why it is considered best practice to close any ports that aren’t associated with a known legitimate service. * We will intensify training measures on this topic. * Ultimately, it's about Awareness rising	When I see that an employee in my department has unnecessary ports open, I send him a picture of Chuck Norris. Whoever has the most pictures at the end of the month has to get the next team breakfast.	In our institution we need the support from the following departments: * HR / PD * IT

Candidate_07_AT: **The main task is to facilitate (physical) data protection for us and our employees.**	We currently have our main computer right at the reception desk (Hotel). Most of the time we don't pay enough attention to log out regularly. This of course represents a security risk, as the open computer is accessible to everyone in the lobby. Therefore we will redesign the small room behind the reception as an office and put the main computer there.	In two weeks we will have finished the room and we will get used to it ourselves, as well as our employees, using this new room, which will be lockable.	In my role as Managing Director, I will strictly ensure that customer data, accounting and other sensitive data are processed exclusively in this separate room.	- Awareness for data protection - Comprehensible translation of the very complex guidelines - Efficient further training for all of us
Candidate_08_AT: **I have to work on a small online solution so that I can easily get a consent form signed** from my suppliers, customers and other companies I work with, in order to properly integrate/publish their data on my website.	I have planned to do a course where I will learn to program simple online forms. In addition, I will meet a privacy expert of a client. Once I have built up the necessary knowledge, I will develop the online form myself or consult a programmer.	This online form should enable my customers, suppliers and cooperation partners to determine in a few minutes which content and data they would like to share via my website for common marketing purposes.	It is my responsibility to ensure that all provisions in the GDPR are complied with. As I said, I will try to build this knowledge as soon as possible.	- Understanding the GDPR (probably with the help of experts in this field) - Programmer - Privacy expert from a client - Awareness rising within my network
Candidate_09_AT: **Have data protection declarations signed by all customers** We have had problems in the past in	In a first step we work on the creation of a clear template, with a short accompanying text, why we	The finished forms are then available at our premises and all employees are trained to	Management control is necessary: we will check that all declarations of our existing	All employees are trained in the basic knowledge of GDPR.

obtaining the necessary explanations and are now working swiftly on implementation.	need this signature from our customers. Then we would like to plan the entire process in detail, from obtaining the necessary signatures - as customer-friendly as possible - to documentation and monitoring.	explain to the customer why their signature is necessary. Should there be any changes to the regulations, we will immediately pass this on to our staff so that they can advise customers well.	customers are available and that new customers are immediately registered in the system.	Communicative skills, especially of our employees with non-German mother tongue, are trained. An information sheet is made available as an aid.
Candidate_10_AT: **Current problem: Clients who keep their accounting records under their desks** It may sound ridiculous, but in addition to our main activities as tax consultants and financial service providers, we are regularly on the road to raising awareness among our clients. Especially small companies and the self-employed make serious mistakes which we constantly point out.	It is not an easy task to point out to clients that they are too careless with their data. We have planned to develop a small brochure that is quick and easy to read, even for clients under time pressure. At the end of this brochure we would like to draw attention to events related to IT security and data protection.	Distribution of the brochure to our clients; answering their specific questions and to inform them, where they can get further training.	During our visits at client's offices, we will keep an eye on whether progress has been made. Awareness rising will probably be important for a long time to come.	Our employees must always be up to date and point out possible dangers to clients. Internally, we must therefore take great care to continuously involve our employees in change processes.

Tasks	Planning Activity	Running Activity	Manage Activity	Skills / knowledge / competencies required
Candidate_01_POL: **to implement a system compliant with the international standard**	• to determine the method • to conduct a risk analysis (it should be remembered that the risk analysis must refer to information security)	the human capital is particularly important in the area of implementation of processes related to information and data security	• the management of continuity with regard to information (the analysis of the most probable and the most severe failures and the development of plans to restore the organization) • all plans created must be periodically tested for suitability at the time the risks materialize	• Readiness to learn • Organization of own work • Creativity • Communication skills • Ability to work in a group • Perseverance • Self-reliance • Sharing knowledge
Candidate_02_POL: **the development of system control tools and increase the scope of control**	coordination of patient care using IT technology	increasing the availability of services and reducing the costs of patient treatment: • implementation of electronic prescriptions, • sending statistical data, • electronic medicine orders, • providing epicrisia and access to the medical history archive (discharge letters), • commissioning laboratory tests and sharing their results (refferals, labresults), • teleradiology, • sharing data with local	• the optimization of control processes is particularly important	• advanced technical skills, both in relation to classic and newer IT departments, such as mobile systems or cloud computing, • the ability to creatively solve problems, • ability to work in a team, • ability to communicate effectively with other people.

		authorities, • management of electronic medical publications.		
Candidate_03_POL: **respecting standards in business processes**	• the risk assessment, aimed at its estimation • ways to minimize the risk	the constant identification of existing threats that may appear at every stage, eg: • application threats (viruses, Trojan horses), • technical failures of the equipment, • cryptographic threats, • communication danger (network overload).	• software tests • monitoring to optimize the effects of activities and use the collected data to create further business plans	communicative skills
Candidate_04_POL: **Identification, analysis and assessment of personal data processing processes**	Designing, maintaining and developing effective processes and controls in the area of information security and data protection in the company.	Providing information, explanations and records for the purposes of audits and reviews to which the company is subject	• Maintenance and development of the Business Continuity Management system • Providing company employees with training and consultation in the field of information security and data protection	• Knowledge of external regulations, standards and good practices in the field of information security and data protection applicable to the company's operations (including: Personal Data Protection Act, GDPR, ISO / IEC 270001, ISO 22301) • Knowledge about data and information management • Ability to work on IT tools and the ability to find areas for improvement and possible errors in the operation of IT tools • Analytical thinking skills • Ability to work under time pressure • Ability to work on many projects at the same time

Candidate_05_POL: **supervision over IT security;**	creating and reviewing internal procedures and regulations;	• participation in the preparation and implementation of security audits; • participation in managing the business continuity plan;	• supervision over IT security; • developing and operating security monitoring systems;	• practical knowledge of network threats and experience in the management and configuration of IT security tools and technologies, practical knowledge and experience in the use of at least two of the following security systems: NG Firewall, IPS / IDS, SIEM, DLP, VPN, MDM; • practical knowledge of network protocols and services, including virtual private networks, and cryptography related issues; • experience in the design, maintenance and verification of the effectiveness of control mechanisms used in the area of IT security; • ability to aggregate information from many sources, prepare analyses, reports, documentation; • analytical and logical thinking skills, comprehensive use of knowledge, organization of own work, communication skills, teamwork skills; • knowledge of standards and procedures regarding information and IT security, including ISO 27000 series standards, KNF recommendations regarding the IT area, GDPR regulation; • knowledge and experience in

				conducting penetration tests
Candidate_06_POL: **Analysis of global company regulations (policies, standards, procedures and instructions) and their adaptation to local conditions.**	• Creating internal policies, standards, procedures and instructions. • Creating the required documentation resulting from security audits. • Creating DRP and BCP. • Preparation of materials and conducting internal training in the field of information security and personal data protection.	• Implementation of created documentation. • Regularly updating existing documentation. • Contact with people responsible for security at the company's headquarters. • Participation in audits (internal and external) and conducting them	Caring for compliance with security auditing requirements.	• Ability to analyse and interpret practical policies and regulations in the area of IT security. • Ability to implement created documentation. • Ability to work with people at various levels of the organization. • Experience in participating and conducting security audits. • Good communication skills. • The ability to look at a topic from a broader perspective. • The ability to convince and defend one's opinion. • Ability to analyse risk. • Knowledge of good practices in IT security and risk management. • Knowledge of ISO standards from the 27000 and 31000 series. • Ability to create DRP and BCP.
Candidate_07_POL: **preparation of draft information on the obligations arising from Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the**	• Development and implementation of educational activities in the area of information security principles, including personal data protection. • Preparation of draft authorization	• Participating in audits of compliance with the GDPR, other EU or Member State data protection laws and internal regulations in the field of personal data	Conducting trainings and instructors in the field of information security rules, including personal data	• Higher education. • Experience in handling cases in the field of personal data protection and / or information security and / or risk management.

protection of individuals with regard to the processing of personal data and on the free movement of such data, and preparing draft opinions in personal data protection.	to process personal data.	protection. • Participate in the data protection impact assessment process. • Keeping a Register of processing activities and a Register of all categories of activities.	protection	• Knowledge of national and European regulations, including GDPR, and practical knowledge of personal data issues. • Competence to share knowledge and experience, • Independence competences, • Analytical thinking skills, Ability to solve problems.
Candidate_08_POL: **identification and analysis of risks in the audited areas**	Creating and implementing target IT security requirements for the company	• Cooperation with external consultants in the creation and implementation of personal data protection requirements in accordance with the EU GDPR • Cooperation with the Risk Director as part of Business Continuity Management	Monitoring the implementation of audit recommendations	• Higher education • Experience in Information Protection and Risk Management • Experience in applying popular IT risk assessment methodologies • Knowledge of ISO / IEC27001, COBiT • CISA, CISM, CIA qualifications • High interpersonal skills, communication skills and creativity • Ability to work in a team • Self-confidence and developed managerial skills • Organizational skills, independence
Candidate_09_POL: **identification of threats to information security**	creating information security system documentation	providing the necessary resources to reduce risks	monitoring threats and incidents in information security	• Education in accordance with the Law on Higher Education and Science • Management experience in higher education • Knowledge of the Law on

				Higher Education and other current sources of law in the field of higher education • Communication skills • Ability to work under time pressure • Good work organization • Availability
Candidate_10_POL: **implementation of the Information Security Policy and related documents**	development and implementation of the Company's Information Security Management System	• conducting proceedings explaining incidents in the field of information security; • cooperation in the field of personal data security with the Personal Data Protection Inspector and the IT System Administrator	• coordination of work related to the preparation, implementation and maintenance of business continuity plans; • checking the correct functioning of the information system in the Company	• higher education; • professional experience in the field of information systems, information security and internal audits; • knowledge of the rules for creating Integrated Security System documentation and documents related to personal data protection